



National Security Agency/
Central Security Service



INFORMATION ASSURANCE CAPABILITIES

DATA AT REST CAPABILITY PACKAGE

Version 3.8
January 2017



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



CHANGE HISTORY

| Title | Version | Date | Change Summary |
|--|---------|----------------|--|
| Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package | 0.8 | July 2014 | Initial draft of CSfC Data-at-Rest (DAR) requirements. |
| Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package | 1.0 | September 2014 | Official release of CSfC DAR requirements. <ul style="list-style-type: none"> Introduced SWFDE/FE (SF) Solution Design Aligned with SW FDE PP 1.0 & FE EP 1.0 |
| Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package | 1.8 | October 2014 | Initial draft of CSfC DAR Version 2 requirements. |
| Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package | 2.0 | December 2014 | Official release of CSfC DAR Version 2 requirements. <ul style="list-style-type: none"> Added PE/FE (PF) Solution Design Aligned with MDF PP 3.0 |
| Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package | 2.8 | May 2015 | Initial draft of CSfC DAR Version 3 requirements. |
| Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package | 3.0 | March 2016 | Official release of CSfC DAR Version 3 requirements. <ul style="list-style-type: none"> Added HWFDE/FE and HWFDE/SW FDE (HF and HS) Solution Design Updated requirements to reflect new FDE Collaborative Protection Profile (cPP) 2.0 Discussed the associated Independent Software Vendor (ISV) technology which aligns with the FDE cPP 2.0 Added Lost and Found (LF) use case. |
| Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package | 3.8 | January 2017 | Initial draft of CSfC DAR Version 4 requirements. <ul style="list-style-type: none"> Added Removable Media (RM) Solution Component and Solution Design Added continuous physical control (previously positive control) guidance Added random password generation, Added secure file deletion guidance, Added optional two-factor authentication. Relocated Threat Section to associated Risk Assessment document |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



TABLE OF CONTENTS

| | | |
|------|---|----|
| 1 | Introduction | 1 |
| 2 | Purpose and Use | 1 |
| 3 | Legal Disclaimer | 2 |
| 4 | Data-at-Rest Protection Overview | 3 |
| 4.1 | Rationale for Layered Encryption | 3 |
| 4.2 | Solution States | 3 |
| 4.3 | DAR CNSA Suite | 4 |
| 4.4 | Authentication | 5 |
| 4.5 | Continuous Physical Control | 7 |
| 4.6 | Lost and Found Use Case | 7 |
| 4.7 | Red, Gray, and Black Data | 8 |
| 4.8 | Cryptographic Erase (CE) | 8 |
| 4.9 | Provisioning | 8 |
| 4.10 | Secure File Deletion | 9 |
| 5 | Solution Components | 10 |
| 5.1 | Software Full Disk Encryption (SWFDE) | 10 |
| 5.2 | File Encryption (FE) | 11 |
| 5.3 | Platform Encryption (PE) | 13 |
| 5.4 | Hardware Full Disk Encryption (HWFDE) | 14 |
| 5.5 | End User Device (EUD) | 16 |
| 5.6 | Removable Media (RM) | 16 |
| 6 | Solution Designs | 16 |
| 6.1 | SWFDE/FE (SF) Solution Design | 17 |
| 6.2 | PE/FE (PF) Solution Design | 18 |
| 6.3 | HWFDE/FE (HF) Solution Design | 18 |
| 6.4 | HWFDE/SWFDE (HS) Solution Design | 19 |
| 6.5 | Removable Media (RM) Solution Design | 19 |
| 7 | Configuration Requirements | 21 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | | |
|------|---|----|
| 8 | Requirements for Selecting Components | 23 |
| 9 | Configuration | 24 |
| 9.1 | Overall Solution Requirements | 24 |
| 9.2 | Configuration Requirements for All DAR Components..... | 25 |
| 9.3 | Requirements for SWFDE Components | 27 |
| 9.4 | Requirements for FE Components..... | 27 |
| 9.5 | Requirements for PE Components..... | 28 |
| 9.6 | Requirements for HWFDE Components | 29 |
| 9.7 | Requirements for End User Devices | 30 |
| 9.8 | Configuration Change Detection Requirements | 34 |
| 9.9 | Requirements for Device Management..... | 34 |
| 9.10 | Auditing Requirements | 35 |
| 9.11 | Key Management Requirements | 36 |
| 9.12 | Supply Chain Risk Management Requirements..... | 36 |
| 9.13 | Lost and Found Requirements | 37 |
| 10 | Requirements Solution Operation, Maintenance, & Handling..... | 39 |
| 10.1 | Requirements for the Use and Handling of Solutions | 39 |
| 10.2 | Requirements for Incident Reporting | 41 |
| 11 | Role-Based Personnel Requirements..... | 43 |
| 12 | Information to Support the AO..... | 45 |
| 12.1 | Solution Testing | 45 |
| 12.2 | Risk Assessment | 46 |
| 12.3 | Registration of Solutions..... | 47 |
| 13 | Testing Requirements | 47 |
| 13.1 | Component Selection..... | 47 |
| 13.2 | End User Device Configurations..... | 48 |
| 13.3 | DAR Component Configuration | 50 |
| 13.4 | Configuration Change Detection..... | 53 |
| 13.5 | Audit..... | 54 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | | |
|---|-----------------------------------|----|
| 13.6 | Key Management | 55 |
| 13.7 | Implementation of Guidance | 55 |
| 13.8 | Incident Reporting Guidance | 57 |
| 13.9 | Solution Functionality | 57 |
| Appendix A. Glossary of Terms | | 58 |
| Appendix B. Acronyms | | 62 |
| Appendix C. CSfC Incident Reporting Template..... | | 66 |
| Appendix D. Password/Passphrase Strength Parameters | | 68 |
| Appendix E: Configuration Guidance | | 71 |
| Appendix F: Continuous Physical control..... | | 77 |
| Appendix G. References..... | | 79 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



LIST OF FIGURES

| | |
|---|----|
| Figure 1: Software Full Disk Encryption | 11 |
| Figure 2: Software File Encryption | 12 |
| Figure 3: Platform Encryption | 14 |
| Figure 4: Hardware Full Disk Encryption | 15 |
| Figure 5: Removable Media Solution Design | 20 |

LIST OF TABLES

| | |
|---|----|
| Table 1: Approved Commercial National Security Algorithm (CNSA) Suite for DAR | 4 |
| Table 2: Solution Design Summary | 17 |
| Table 3: Requirement Digraphs | 22 |
| Table 4: Product Selection Requirements | 23 |
| Table 5: Overall Solution Requirements | 24 |
| Table 6: Configuration Requirements for All DAR Components | 25 |
| Table 7: Requirements for SWFDE Components | 27 |
| Table 8: Requirements for FE Components | 27 |
| Table 9: Requirements for PE Components | 28 |
| Table 10: Requirements for HWFDE Components | 29 |
| Table 11: Requirements for End User Devices | 30 |
| Table 12: Configuration Change Detection Requirements | 34 |
| Table 13: Requirements for Device Management | 34 |
| Table 14: Auditing Requirements | 35 |
| Table 15: Key Management Requirements for All DAR Components | 36 |
| Table 16: Supply Chain Risk Management Requirements | 36 |
| Table 17: Lost and Found Requirements | 37 |
| Table 18: Requirements for the Use and Handling of Solutions | 39 |
| Table 19: Incident Reporting Requirements | 41 |
| Table 20: Test Requirements | 46 |
| Table 21: Randomly Generated Minimum Password Length | 69 |
| Table 22: Randomly Generated Minimum Passphrase Length | 70 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY





Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency (NSA) Information Assurance (IA) Capabilities Directorate publishes Capability Packages (CP) to provide architectures and configuration requirements that empower IA customers to implement secure solutions using independent, layered Commercial Off-the-Shelf (COTS) products. The CPs are product-neutral and describe system-level solution frameworks documenting security and configuration requirements for customers and/or Integrators. It is recommended that CSfC Trusted Integrators be employed to architect, design, integrate, test, document, field, and support the solution. The list of CSfC Trusted Integrators can be found at:

https://www.nsa.gov/ia/programs/csfc_program/trusted_integrators_list.shtml.

This generic CSfC Data-at-Rest (DAR) CP meets the demand for DAR solutions using Commercial National Security Algorithm (CNSA) CNSA Suite. These algorithms are used to protect classified data using layers of COTS products. The DAR CP Version 3.8 enables customers to implement two independent layers of encryption for the purpose of providing protection for stored information while the End User Device (EUD), defined in Section 5.5, is powered off or in an unauthenticated state. This CP takes lessons learned from one proof-of-concept demonstration per solution design that has implemented the CNSA Suite, modes of operation, standards, and protocols. These demonstrations included a layered use of COTS products for the protection of classified information.

While CSfC encourages industry innovation, trustworthiness of the components is paramount. Customers and their Integrators are advised that modifying a National Information Assurance Partnership (NIAP)-validated component in a CSfC solution may invalidate its certification and require a revalidation process. To avoid delays, customers and Integrators who feel it is necessary to modify a component should engage the component vendor and consult NIAP through their Assurance Continuity Process (https://www.niap-ccevs.org/Documents_and_Guidance/ccevs/scheme-pub-6.pdf) to determine whether such a modification will affect the component's certification.

In case of a modification to a component, NSA's CSfC Program Management Office (PMO) will require a statement from NIAP that the modification does not alter the certification, or the security of the component. Modifications that will trigger the revalidation process include, but are not limited to: configuring the component in a manner different from its NIAP-validated configuration, and modifying the Original Equipment Manufacturers' (OEMs') code (to include digitally signing the code).

2 PURPOSE AND USE

This CP provides high-level reference designs and corresponding configuration requirements that allow customers to select COTS products from the CSfC Components List available on the CSfC web page (http://www.nsa.gov/ia/programs/csfc_program), for their DAR solution and then to properly configure those products to achieve a level of assurance sufficient for protecting classified data while at rest. As



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



described in Section 8, customers must ensure that the components selected from the CSfC Components List will provide the necessary functionality for the selected capabilities. To successfully implement a solution based on this CP, all Threshold Requirements, or the corresponding Objective Requirements applicable to the selected capabilities, must be implemented, as described in Sections 7 - 12.

This document, the CSfC Data-at-Rest CP Version 3.8, dated February 2017, has not been approved by the Deputy National Manager for National Security Systems and is being released solely for the purpose of soliciting public comments.

Please provide comments on usability, applicability, and/or shortcomings to your NSA/IA Client Advocate (CA) and the DAR Capability Package maintenance team at CSfC_DAR_team@nsa.gov. DAR CP solutions must also comply with the Committee on National Security Systems (CNSS) policies and instructions. Any conflicts between CNSS or local policy and this CP should be provided to the DAR CP Maintenance team.

Additional information about the CSfC process is available on the CSfC web page (www.nsa.gov/ia/programs/csfc_program).

3 LEGAL DISCLAIMER

This CP is provided “as is.” Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States (U.S.) Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this CP, even if advised of the possibility of such damage.

The User of this CP agrees to hold harmless and indemnify the U.S. Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney’s fees, court costs, and expenses, arising in direct consequence of recipient’s use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of user or third parties, damage to or destruction of property of user or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer’s product or service.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



4 DATA-AT-REST PROTECTION OVERVIEW

The goal for the DAR solution is to protect classified data when the EUD is powered off or unauthenticated. Unauthenticated, in this case, means prior to a user presenting and having their credentials (e.g., password, tokens, etc.) validated by both layers of the DAR solution. Specific data to be protected must be determined by the data owner.

4.1 RATIONALE FOR LAYERED ENCRYPTION

A single layer of CNSA encryption, properly implemented, is sufficient to protect classified DAR. The DAR solution uses two layers of CNSA encryption not because of a deficiency in the cryptographic algorithms, but rather to mitigate the risk that a failure in one of the cryptographic components: by accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability, results in the exposure of classified information. The use of multiple layers, implemented with components meeting the CSfC vendor diversity requirements, reduces the likelihood that a single vulnerability can be exploited to reveal protected information.

If one of the encryption layers is compromised or fails in some way, the second layer can still provide the needed encryption to safeguard the classified data. If both layers are compromised or fail simultaneously, it is possible the classified data will become readable to a threat actor. The goal of the DAR solution is to provide redundant protection that either minimizes the possibility of both layers failing at the same time or requires an adversary to defeat both mechanisms.

4.2 SOLUTION STATES

The DAR solution states are identified and described in further detail in this section. Note that once a device is considered classified (e.g., Powered-On with Outer Layer Authenticated State) it will not be considered unclassified (must still be handled in accordance with the implementing organizations' Authorized Official (AO) policies again until the device is powered-down.

Powered-Off State:

In a powered-off state, the device is completely off and not in any power saving state. The EUD is considered unclassified, but must still be handled in accordance with the implementing organizations' AO policies. This includes all removable media when unplugged from the host system.

Powered-On and Unauthenticated State:

In a powered-on and unauthenticated state, the EUD is completely on, but the user has not initially logged into either layer. The EUD is considered unclassified, but must be handled in accordance with the implementing organizations' AO policies. This state cannot be entered by logging off after initial logon. This includes all removable media when plugged into the host system.

Powered-On with Outer Layer Authenticated State:



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



In a powered-on state with outer layer authenticated, the device is operational where the user has authenticated to the outer layer of encryption. The device in this state is considered classified and should be handled accordingly. This includes all removable media when plugged into the host system.

Powered-On with Outer and Inner-Layer Authenticated State:

In a powered-on state with outer and inner-layer authenticated, the EUD is operational when the user has authenticated to two layers of DAR encryption. The device in this state is considered classified and should be handled accordingly. This includes all removable media when plugged into the host system.

Locked State:

In a locked state, the device is powered-on but most of the functionality is unavailable for use. User authentication is required to access functionality. This functions as an access control and may provide one layer of DAR protection. The device in this state is considered classified and should be handled accordingly. This includes all removable media when plugged into the host system.

4.3 DAR CNSA SUITE

As the portability of EUDs increases, the requirements for when and how classified data is protected also increases. EUDs can be used in both physically protected and physically unprotected environments. Solutions using commercial products must protect classified data on the EUD by using two layers of encryption with the approved CNSA Suite.

Table 1: Approved Commercial National Security Algorithm (CNSA) Suite for DAR

| Security Service | CNSA Suite Standards | Specifications |
|------------------------------------|---|----------------|
| Confidentiality (Encryption) | AES-256 | FIPS PUB 197 |
| Authentication (Digital Signature) | ECDSA over the curve P-384 with SHA-384 | FIPS PUB 186-4 |
| | RSA 3072 (Minimum) | FIPS PUB 186-4 |
| Integrity (Hashing) | SHA-384 | FIPS PUB 180-4 |
| Can protect | Up to Top Secret | ----- |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



IA will initiate a transition to quantum resistant algorithms in the not too distant future. IA customers using layered commercial solutions to protect classified national security information with a long intelligence life should begin implementing a layer of quantum resistant protection. Such protection may be implemented today through the use of large symmetric keys coupled with specific secure protocol standards. For more information please go to http://www.nsa.gov/ia/programs/suiteb_cryptography/.

The solutions presented in this CP have specific requirements for configuration, product selection, components, provisioning, authentication, key management, operations, administration, roles, use and handling.

The DAR CP is focused on the implementation of cryptography to mitigate the risk to classified data from unauthenticated access when the device is powered off or unauthenticated. This CP does not protect against malicious code exploits and potential vulnerabilities from updates, operating system (OS) misconfigurations, or the persistence of remnants of key or plaintext material in volatile memory on the EUD when powered on, as these conditions are outside of the scope for this version of the CP because they are not considered in current protection profiles (PP).

4.4 AUTHENTICATION

In the capability package, each layer is required to have a “known secret” (i.e. PIN, password, or passphrase), smartcard, or USB token to authenticate to each of the two encryption layers. The permitted factors may differ based on the layer. DAR encryption products must meet requirements for each of these factors during evaluation against the applicable protection profile. These are considered primary (validated) authentication factors for that component.

Many products offer alternate authentication mechanisms. When implementing the DAR solution, these alternate mechanisms may be used only as a secondary (non-validated) authentication factor and must be paired with a primary authentication factor. Secondary factors may act as an additional access control or may contribute to the products key chain; the products protection profile evaluation guarantees there is no loss in strength when combining keys with potentially weaker sources. A layer may use any number of authentication factors as long as one is a primary factor as listed in that component’s specific authentication requirement. As an example, layer one may use a known secret (primary factor) along with a biometric (secondary factor), and layer two may use a smartcard. It is important to consider the requirements, benefits, and drawbacks associated with different authentication factors. Some considerations of popular factors are discussed below.

Known secrets are memorized values that can provide a strong authentication value if well chosen (see Appendix A) and are typically supported by almost all products. They are at risk of being forgotten, as well as being seen while being keyed into the device. The majority of the time, known secrets will be weaker than tokens and are at risk of being very weak if not properly chosen.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



Smartcard tokens are small integrated circuit devices that can store authentication keys. As long as they are handled and stored properly, they provide a very strong form of authentication. They provide a flexible option for authenticating a user to many devices and providing additional security through the use of a PIN to use the card. Aside from the benefits, cards are susceptible to loss and damage. In addition, they may also require a separate system for provisioning and recovery.

USB tokens are a simple form of token that provide a very strong form of authentication as long as they are handled and stored properly. Although very easy to provision, they generally have no additional security features, unless the USB device itself provides those features. Unfortunately they are not permitted in many places.

Biometric technology functions by taking a measurement of an element of the user's body. Common examples are fingerprints, iris scans, and facial recognition. This measurement is compared against a template that is created during provisioning; if the measurement matches the template, the user is authenticated. The vendor may use this authentication as an access control or they may release a key to contribute to decryption. If a key is used, it will be important to ask how that key is protected and what authorizes the key's release, as there are currently no methods being used to derive a biometric measurement into a key. When using biometrics there may be instances when an unauthorized user will be authenticated to the biometric when they should not, this is called a false acceptance and a condition with which all biometrics have to contend. Customers should obtain vendors' false acceptance rates and determine how comprehensive their testing was to determine that rate. The other rate to address is the false rejection rate, which is when an authorized user's measurements fail to authenticate. This is a usability concern and should also be discussed with the vendor. The biometric template used to compare measurements is intended to be constructed so that the user's measurements are not reversible. If an adversary was able to obtain the template, they would be unable to reconstruct the user's fingerprint. However, this is not always the case; templates are not well standardized and there have been cases of reconstruction. This may be a risk to the privacy of users. One of the major risks of biometric is spoofing. This involves using other technology to recreate the user's measurement. Examples of spoofing include taking photos of the user's face or lifting fingerprints. The vendor should explain how they mitigate spoofing and users should protect the area being used to authenticate. Many biometrics need a fallback mechanism in case the area being used to authenticate to the biometric system becomes damaged, such as a finger being cut. Consideration should be given to what the fallback mechanism is or the consequences if there is none.

Near field communication is a short range signal. Generally the devices are bumped together to exchange information in this method. This signal can vary in how it is used during the authentication process. There may be an exchange of key material or there may not. The details of what is exchanged will need to be discussed with the vendor. Regardless of what is exchanged, the devices should be kept separately and treated like a Smartcard or USB token. This may not be permitted if used in conjunction with other CPs.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



Behavior based authentication covers a wide variety of features. The goal is to identify if an authorized user has the device, based on whether the device is being used and handled the way the authorized user normally uses the device. Based on this information the device may release a key, provide an access control, or allow for a longer time before locking the device. Some factors it may take into account are location, connected networks, gyroscope measurements, user interaction, and other internal sensors.

4.5 CONTINUOUS PHYSICAL CONTROL

Although the DAR solution can protect the confidentiality of data and render the EUD or Removable Media (RM) unclassified, it does not protect the integrity of an EUD outside of the control of approved users. It is difficult to examine and determine whether or not a device has been tampered with; therefore, the EUD must remain in continuous physical control at all times. The NSA requires that implementing organizations define the circumstances in which an EUD that is part of the solution is considered outside of the continuous physical control of authorized users (i.e., "lost"). Authorizing Officials (AO) will define "continuous physical control", and this definition should align with the intended mission and threat environment for which the solution will be deployed. Each organization must also define the circumstances in which an EUD that is a part of its solution is to be considered recovered back into the continuous physical control of authorized users (i.e., "found").

This CP requires any lost device, once found, to be rigorously investigated and/or destroyed in order to mitigate threats to the integrity of the EUD and any connected systems, because upon being found, the device is considered not secure unless the device meets lost and found requirements (see Section 9.13). AOs should consult the DAR CP Risk Assessment (RA) to help make an informed risk decision.

See Appendix F for additional requirements information and some examples of continuous physical control.

4.6 LOST AND FOUND USE CASE

The "lost and found" (LF) use case is when a user, intentionally or unintentionally, temporarily loses control of a device (as defined by the AO) and plans to continue using it after it is recovered. This use case adjusts the continuous physical control requirements from Section 4.5 and permits the device to be used after it is found; however if the device is suspected to have been tampered with, it must be rigorously investigated and/or destroyed.

This use case is intended to cover situations including but not limited to: devices left in vehicles or devices forgotten in hotels for short periods of time, going through customs, and similar events. These requirements lower the risk of using devices that have been in such conditions, but they do not eliminate the risk. With this in mind, AOs should consider additional local policy to reduce the situations where devices may be vulnerable to tampering.

This use case also contains a requirement to personalize the EUD. The intent of the personalization requirement is to ensure that if an adversary removed the EUD and replaced it with another EUD of the same make and model, it would be noticed by the end user. Personalization includes: adding stickers,



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



changing the screen's background, etc. The administrator may also change settings to personalize the devices for subsets of users, such as login screen wallpaper. None of these changes should undermine any security features of the device or other relevant security policy (e.g., such as requiring the device to be rooted).

4.7 RED, GRAY, AND BLACK DATA

This CP uses the following terminology to describe the data types that compose a DAR solution. The terms Red, Gray, and Black identify the number of encryption layers applied to classified data for a specific EUD state.

Red data is unencrypted classified data being processed by the EUD. After a user successfully authenticates to the outer and inner layers of DAR encryption, the EUD is in a state of processing Red data.

Gray data contains classified information that has been encrypted once. After a user successfully authenticates to the outer layer of DAR encryption, but has not yet authenticated to the inner layer of encryption, the EUD is in a state of processing Gray data.

Black data contains classified information that has been encrypted twice. An EUD is considered black when the device is powered off and/or unauthenticated and the stored data has been encrypted with both the outer and inner layers of DAR encryption.

4.8 CRYPTOGRAPHIC ERASE (CE)

CE is a method of sanitization in which an encryption key for the encrypted data is sanitized, making recovery of the decrypted data infeasible. In this document it is used to ensure clean re-provisioning, as an additional protection triggered by failed authentication, or as an emergency method of sanitizing the media if proper destruction methods cannot be met (see DAR-EU-2 in Table 11).

4.9 PROVISIONING

Provisioning is the process through which EUDs are initialized before first use. During the provisioning process, the Security Administrator (SA) loads and configures the DAR components for the EUD. Provisioning is inherently an out-of-band process requiring physical access to the EUD. The DAR solution cannot be applied to an EUD that already has data stored on it.

EUD re-provisioning or reuse of DAR components is allowed as long as it is performed in accordance with this CP. If re-provisioning, the EUD must be at the same or higher classification level of the previous unencrypted data stored on the approved DAR solution. Re-provisioning EUD components from any non-CSfC solution is prohibited.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



4.10 SECURE FILE DELETION

When deleting files via normal means (i.e. deleting followed by emptying the recycle bin, shift + delete, etc.) from the computer, there is a possibility for residual data to remain on the underlying storage media for extended periods of time, recoverable by forensic techniques. While the DAR CP requires multiple layers of encryption and tries to mitigate user error, it is still possible for the device to be compromised, in that event securely deleting files reduces the information available to the adversary. For these reasons, it is recommended to use applications to securely delete files.

Secure file deletion tools make use of more direct methods to mitigate the risk of data being recoverable. Since there is not currently a method of validation for providing secure file deletion, here are some recommendations for features to include when acquiring a secure file deletion product. When looking for a product to fulfill this purpose, the type of storage media must be considered. There are currently two primary storage drives used today, hard disk drives (HDD) and solid state drives (SSD). Flash USB drives fall into the same area as SSDs.

Normally when a file is deleted from an HDD the reference to that file's content is removed. The majority of the data will continue to reside on the disk, being treated as free space for new data to use. This makes the role of a third party product straightforward. It should claim to directly overwrite the file reference and file data with any value that would not contain sensitive data, such as the contents of RAM. Products may provide options for performing multiple passes although this is not necessary, as a single pass provides sufficient security; however if only multiple passes are supported, they will not cause any harm.

In order to understand the residual risk, it is important to understand the basics of the complications involved in erasing memory from an SSD. There are two major complications for deleting data on solid state. The first issue is that the memory used is not highly reliable. To address the reliability problem an SSD will have more storage than is directly accessible by the user. This storage is used to keep additional copies of data and provide error correction. The second is that in drives when a user deletes a file, the drive will mark that area as free space, but will not actually overwrite the data. This is for performance reasons, the memory used by the SSD must be cleared before being written to again and that takes time. The drive works in conjunction with the operating system to perform this task in the background when the drive does not have more important tasks. Because of these issues it is not possible for a third party file deletion tool to directly overwrite data. There is also an upside, which is regular deletion can result in a direct overwrite eventually unlike HDDs where the data can remain for long periods of time. Because of this third party tools are not necessary, and files may be deleted via normal means. However, there are other factors that affect the SSD drives background overwrite process from taking place. The restrictions below detail configurations over which a user can exert control. There are other situations where a user cannot exert control, which has the potential to result in data residing on the SSD for an extended undefined period of time. This is acceptable since any residual data should be encrypted. If any of the restrictions below apply, some third party products may be able to overcome



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



them. Otherwise the product should ensure the SSD clears memory as soon as possible, issuing commands to the drive to enable that.

- TRIM, the command issued to the SSD to clear space, may not be supported by the operating system. Most modern operating systems do support this command, check operating system documentation to ensure support for TRIM.
- The TRIM command may only be supported by the OS if certain file systems are being used. Check vendor documentation to ensure a compatible file system is used.
- The way this is checked varies between operating systems. Check operating system documentation on how to verify TRIM is enabled.
- Older SSDs may not support the TRIM command. The majority of modern drives do have support, check vendor documentation to ensure the device supports this command.
- The operating system may not support TRIM for external drives, USB flash drives, or other devices connected over USB, PCI E, M.2 and other interfaces. This is a common area where a third party product may provide additional benefit.
- The operating system may not support TRIM when a RAID configuration is used.

DAR products that support encrypted volumes may interfere with the TRIM command for data within the volumes. Some products do enable TRIM to function within the encrypted volumes, check vendor documentation for verification.

5 SOLUTION COMPONENTS

This section describes the capabilities of each component. Section 6 describes the possible functional implementations of each component within the possible Solution Designs and summarizes them in Table 2.

5.1 SOFTWARE FULL DISK ENCRYPTION (SWFDE)

SWFDE, shown in Figure 1, is used to provide one layer (either the inner or outer layer depending on the solution implemented) of DAR protection. The National Institute of Standards and Technology (NIST) Special Publication 800-111 “Guide to Storage Encryption Technologies for End User Devices” defines full disk encryption as follows: “Full Disk Encryption (FDE), also known as whole disk encryption, is the process of encrypting all the data on the drive used to boot a computer, including the computer’s OS, and permitting access to the data only after successful authentication to the FDE product.” A user must log into the Pre-Boot Environment (PBE) with valid credentials. Once the user is authenticated to the PBE, the SWFDE decrypts and boots the OS.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY

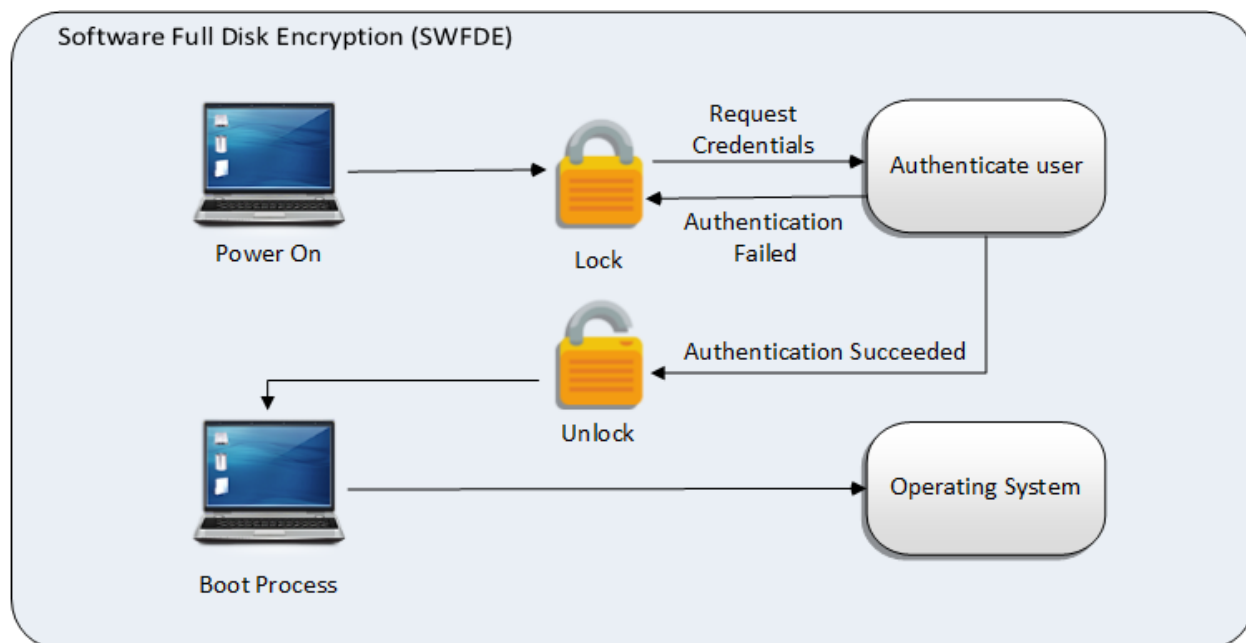


Figure 1: Software Full Disk Encryption

5.2 FILE ENCRYPTION (FE)

FE, shown in Figure 2, is approved to provide the inner layer of DAR protection. FE is the process of encrypting individual files or sets of files on an EUD and permitting access to the encrypted data only after proper authentication is provided.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY

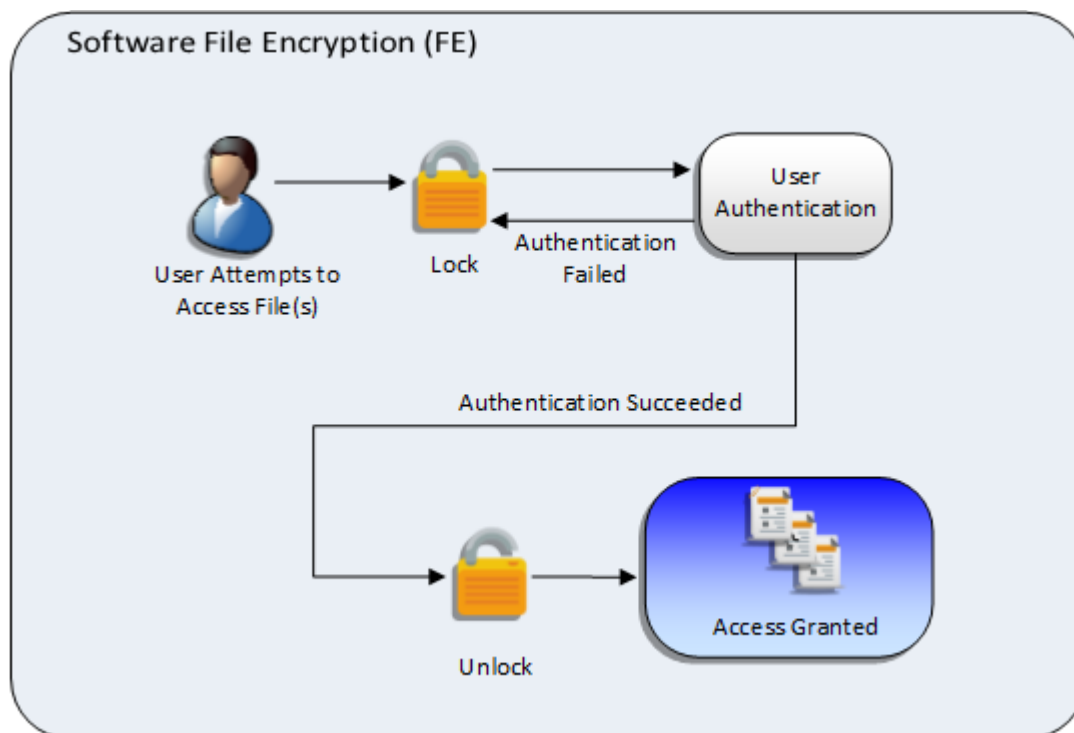


Figure 2: Software File Encryption

FE products currently on the market have a wide range of implementations. It is important for the user to understand how a specific FE product operates to ensure all classified data on the EUD is encrypted. There are many events and applications that may write data to the disk. Users should be made aware of these through user training unless the FE product can encrypt the data without their intervention. Some examples of such events are:

1. Applications permitted to run on the EUD should be carefully considered. Applications may create files (e.g., temporary files) in unprotected locations leaving classified data at risk. If an application (e.g., file viewer) will be interacting with sensitive data and is not protected by an FE component, that application must be evaluated against the Application Software Protection Profile (ASPP) and meet the selection “not store any sensitive data” in FDP_DAR_EXT.1.1.
2. Paging files (e.g., swap files) are created when the system runs out of or becomes low on unused volatile memory, also known as Random Access Memory (RAM). When this occurs, the system may write to the non-volatile memory (e.g., hard disk) for storage. If the product cannot automatically protect this data, the solution should disable system page files.
3. Systems restore, and other features that allow data to be restored to a previous point in time create copies of the data. If this is enabled, it may allow an encrypted file to be restored to a



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



state before it was encrypted. Unless the product accounts for these types of scenarios, these features should be disabled.

4. Memory dump files may be created when an error occurs. Memory dump files may include classified data that existed in volatile memory when the crash occurred. Since these files are created during a system crash, it is likely the product will not be able to properly encrypt them. Therefore, it is recommended this feature be used with care by individuals who understand what data will be contained within the file or the feature should be disabled.
5. Printer spool files are created when a document is sent to print. These are used to hold documents while they are in queue for printing. If the solution is going to print any classified information, these files should be protected.
6. Moving or deleting files: users should be informed that moving (cut/paste) a classified file into a protected area is not sufficient for protecting it. Moving or deleting a file while it is unencrypted may leave file contents on the disk until it is overwritten by the file system. This should apply to all file movement for good practice, even though it would not apply in all cases. All files should be encrypted before being deleted or moved.

FE protects the confidentiality of individual files, folders, or volumes, and may be accomplished in several ways. The encryption may be performed by an application, platform, or the host OS. Each encrypted file, folder or volume will be protected by a File Encryption Key (FEK). The FEK is protected by the user's authentication factor, either directly or through one or more Key Encryption Keys (KEKs).

Proper user authentication is required to decrypt the FEK. The FE product will then decrypt files or folders on an individual basis as they are requested by the user via specific applications. To ensure that no classified data is left unprotected, the AO shall be responsible for providing and enforcing a policy that mandates automation and user compliance to encrypt all classified data.

5.3 PLATFORM ENCRYPTION (PE)

PE, shown in Figure 3, is approved to provide the outer layer of DAR protection. PE is provided by the OS for platform-wide data encryption, transparently encrypting sensitive user data. The PE layer requires hardware-backed secure key storage, with the goal of reducing the need for long and complex passwords. With the exception of the hardware-specific requirements and which layer they can be used for (PE protects the outer layer while FE protects the inner layer), there is little distinction between PE and FE implementations. In all other respects, the two component implementations are virtually identical; they both provide volume and FE capabilities.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY

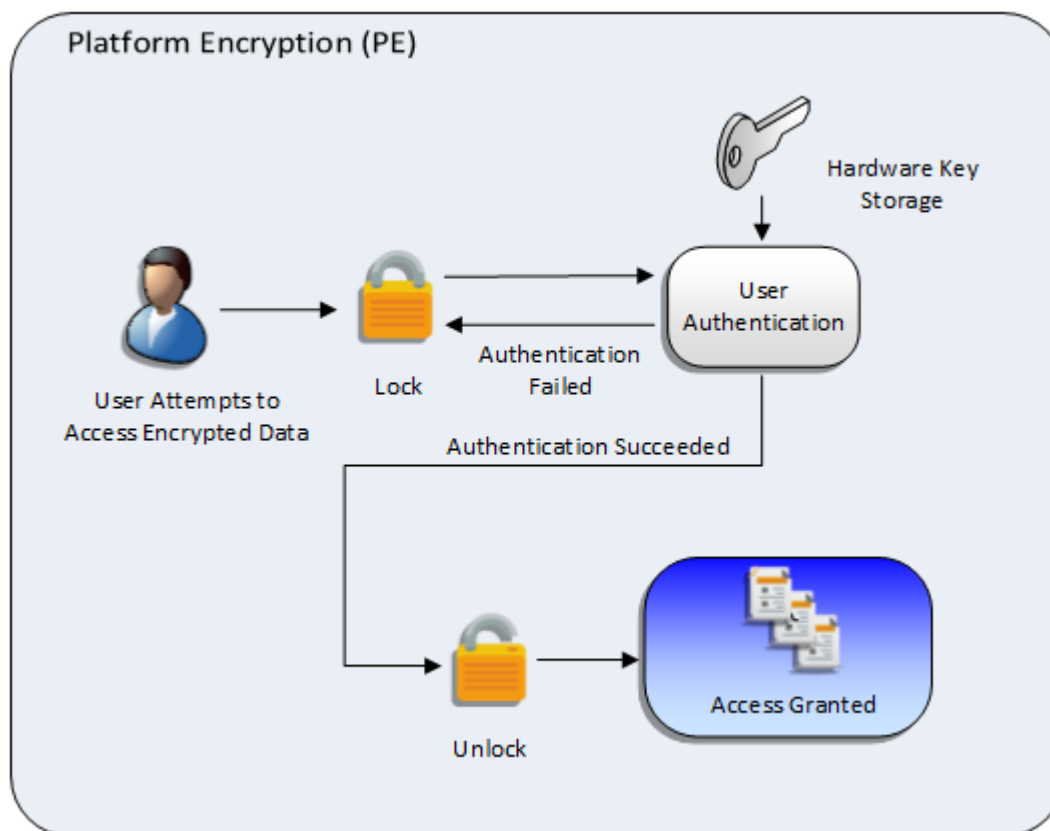


Figure 3: Platform Encryption

The PE solution relies on the EUD to implement the requirements specified in the Mobile Device Fundamentals (MDF) PP along with the CSfC selected requirements. Items that meet the NIST requirements for PE solutions are located in the CSfC Components List under Mobile Platform.

5.4 HARDWARE FULL DISK ENCRYPTION (HWFDE)

HWFDE, shown in Figure 4, can be used to provide the outer layer of DAR protection. HWFDE is commonly implemented via a Self-Encrypting Drive (SED). The SED can be a standard hard drive or a Solid State Drive (SSD).



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY

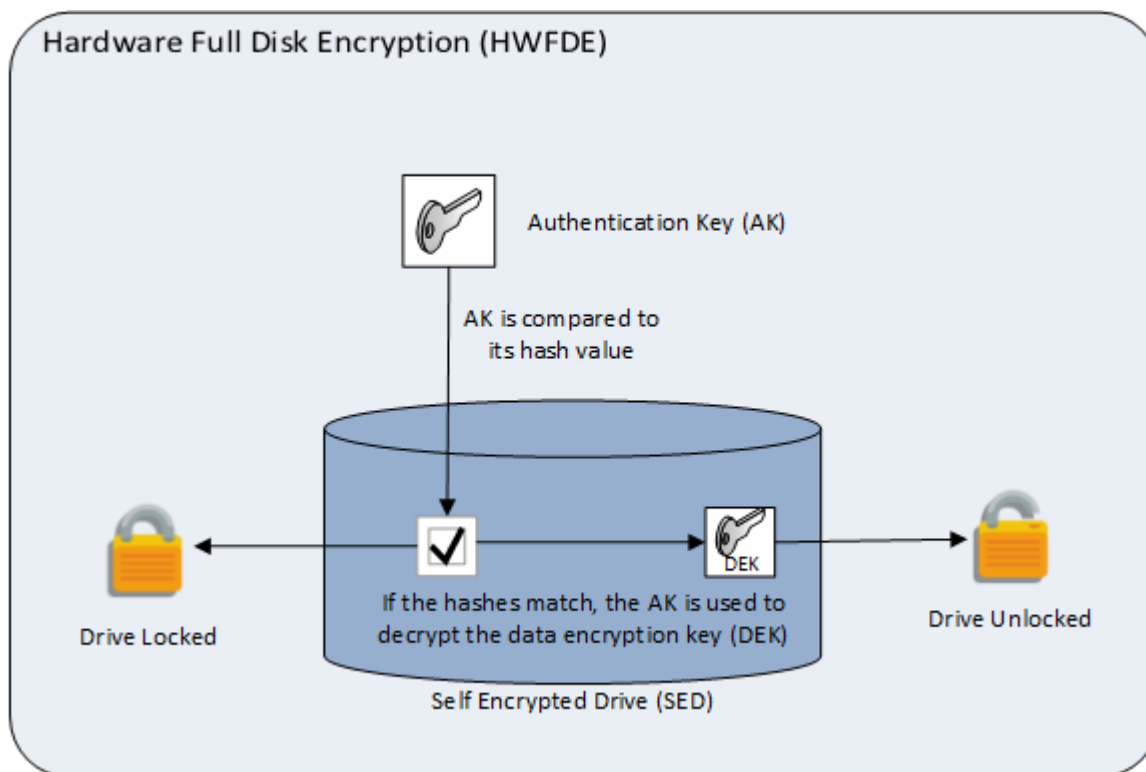


Figure 4: Hardware Full Disk Encryption

A SED contains hardware built into the drive controller chip that automatically encrypts all data written to the drive and decrypts all data read from the drive. The encryption and decryption is done transparently to the user.

In some cases, the HWFDE solution will require multiple components to create an FDE solution. Some SEDs require a product from an Independent Software Vendor (ISV) to function; this ISV commonly fills the role of collecting initial authentication and passing it to the SED. It is essential that both parts of the solution are chosen from the CSfC Components List.

The Authentication Key (AK) used in HWFDEs to encrypt or decrypt data is called the Data Encryption Key (DEK), which is protected by a chain of keys originating from the authentication factor.

A user must log into the PBE, provided by the SED or an ISV, with valid credentials. Once the user is authenticated to the PBE, the HWFDE decrypts and boots the operating system.

When discussing the use of ISVs and SEDs, the relevant information is sometimes referred to as FDE AA & EE breakout information.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



5.5 END USER DEVICE (EUD)

The EUD is either: a personal computer (e.g., desktop, laptop); consumer device (e.g., smart phone, tablet); or a server (e.g., storage area network, network area storage, shared drives, external storage). It is important to keep the security of different power states in mind when using these devices. An EUD may operate within a secure physical environment, outside of a secure physical environment, or both inside and outside of a secure physical environment as approved by the AO.

The drives that make up a Storage Area Network (SAN) or a Network Area Storage (NAS) can be protected via the solutions presented in this CP, but that protection is provided only when the system is powered off (i.e., no solutions presented in this CP provide protection to SAN/NAS systems while the system is powered on). For powered on scenarios, consult the Mobile Access or Campus Wireless LAN Capability Package on the CSfC web site.

5.6 REMOVABLE MEDIA (RM)

In this CP, a removable medium is defined as a device which has the primary purpose of providing external storage of data protected by DAR through implementing two layers of encryption. Removable media can include: a USB drive, a microSD card, or a removable drive. This use case allows customers to transfer data using an external storage device between different systems or expand the storage of a single system. For example, this use case can be used to transport data via a removable media device between secured facilities, using a DAR CP compliant solution on both ends. This requires using two approved layers of encryption on the RM device that is provisioned within a secured facility, then transporting the RM under continuous physical control to access data on a DAR CP compliant workstation or device.

6 SOLUTION DESIGNS

The CP provides the multiple solution designs listed in Table 2. The designs describe solutions meeting a wide variety of requirements to protect classified DAR.

The “SF” design consists of SWFDE and FE. The SF architecture is typically intended for EUDs such as servers, desktops, laptops, and tablets.

The “PF” design consists of PE and FE. The PF architecture is typically intended for EUDs such as laptops, tablets, and smart phones.

The “HF” design consists of HWFDE and FE. The HF architecture is typically intended for EUDs such as servers, desktops, laptops, and tablets.

The “HS” design consists of HWFDE and SWFDE. The HS architecture is typically intended for EUDs such as servers, desktops, laptops, and tablets.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



The “RM” design consists of either the SF, HF or HS architecture on removable media such as USB drives, microSD cards and removable drives. If RM is part of the design the solution must comply with requirements that meet both the RM and the additional solution design requirements. If a solution includes both host machines and RM, the customer must submit the registrations separately.

Table 2: Solution Design Summary

| Solution Design | Designator | Description |
|------------------------|-------------------|---|
| SWFDE/FE | SF | DAR solution design that uses FE as the inner layer and SWFDE as the outer layer, as described in Section 6.1. |
| PE/FE | PF | DAR solution design that uses FE as the inner layer and PE as the outer layer, as described in Section 6.2. |
| HWFDE/FE | HF | DAR solution design that uses FE as the inner layer and HWFDE as the outer layer, as described in Section 6.3. |
| HWFDE/SWFDE | HS | DAR solution design that uses SWFDE as the inner layer and HWFDE as the outer layer, as described in Section 6.4. |
| RM | RM | DAR solution design that uses RM through the use of a SF, HF, or HS solution design as described in Section 6.5. |

The solution is contained in an individual EUD. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible solution owners must implement the Threshold version of the requirement instead.

6.1 SWFDE/FE (SF) SOLUTION DESIGN

The SF solution design requires SWFDE and file/folder/volume encryption. In the SF solution design, SWFDE will be used to provide DAR protection for the outer layer and FE will be used to provide DAR protection for the inner layer. The SF DAR solution uses a password, passphrase, smartcard or Universal Serial Bus (USB) token to provide access to classified data. Once a user inputs the correct password, passphrase, smartcard token or USB token, the system boots the operating system. Next, the user authenticates to the FE, which in turn decrypts the user’s classified files.

Each layer of encryption in the SF DAR solution may use similar authentication mechanism types (e.g., passwords, passphrases, or tokens) but requires a unique authentication credential for each layer. For the first layer of encryption, the user will authorize to the PBE provided by the SWFDE. For the second layer, the user will use their OS login credentials, application credentials, or file-specific credentials to authenticate to the FE.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



6.2 PE/FE (PF) SOLUTION DESIGN

The PF solution design permits platform encryption and file/folder/volume encryption. In the PF solution design, PE will be used to provide DAR protection for the outer layer and FE will be used to provide DAR protection for the inner layer. The PF solution uses passwords to provide access to classified data. Once a user inputs the correct password, the platform is decrypted, which then provides access to user data. Next, the user authenticates to the FE, which in turn decrypts the user's classified files. Each layer of encryption in the PF DAR solution may use similar authentication mechanism types (e.g., passwords) but requires a unique authorization credential for each layer.

The second layer in the PF architecture can be implemented in different ways and should be part of the design considerations when implementing this solution. The FE layer can be implemented in one of two options as described below:

1. The first option is provided by the platform if, and only if, appropriate cryptographic separation and independence can be ensured in accordance with CSfC principles. Most of the available FE solutions are implemented on a per application basis. This approach may have an impact on user experience, since the user must independently authenticate to each application providing FE solutions. For Information Assurance (IA)-enabled applications, this method of implementation would require each application to be evaluated against the ASPP with File Encryption Extended Package (FE EP).
2. The second option is provided by an application container. An application container may be used to protect the data from multiple applications. This would reduce the number of IA-enabled applications that would need to be evaluated against the ASPP with FE EP at the expense of ensuring integration of each client application with the container.

6.3 HWFDE/FE (HF) SOLUTION DESIGN

The HF Solution Design requires hardware full disk encryption and file/folder/volume encryption. In the HF solution design, HWFDE will be used to provide DAR protection for the outer layer and FE will be used to provide DAR protection for the inner layer. The HF DAR solution uses a password, passphrase, smartcard, or USB token to provide access to classified data. Once a user inputs the correct password, passphrase, smartcard, or USB token, the system boots the operating system. Next, the user authenticates to the FE, which in turn decrypts the user's classified file.

Each layer of encryption in the HF DAR solution may use similar authentication mechanism types (e.g., passwords, passphrases, smartcard, or USB token) but requires a unique authentication credential for each layer. For the first layer of encryption the user will authenticate to the PBE provided by the HWFDE. For the second layer the user will use their OS login credentials, application credentials, or file-specific credentials to authenticate to the FE.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



6.4 HWFDE/SWFDE (HS) SOLUTION DESIGN

The HS solution design approach requires hardware full disk encryption and software full disk encryption. In the HS solution design, HWFDE will be used to provide DAR protection for the outer layer and SWFDE will be used to provide DAR protection for the inner layer. The HS DAR solution uses a password, passphrase, smartcard or USB token to provide access to classified data. Once a user inputs the correct password, passphrase, smartcard or USB token value, the HWFDE allows the booting of the operating system. The operating system will then require the user to authenticate to the SWFDE, after which the user has access to the data on the drive.

Each layer of encryption in the HS DAR solution may use similar authentication mechanism types (e.g., passwords, passphrases, or tokens) but requires a unique authentication credential for each layer. For each layer of encryption the user will authenticate to a PBE provided by the HWFDE and SWFDE, respectively.

6.5 REMOVABLE MEDIA (RM) SOLUTION DESIGN

The RM use case, shown in Figure 5, requires two layers of encryption to be employed on the removable media device/form factor. This use case allows customers to use an external storage device between different systems to protect DAR and has different password requirements. In the RM solution design, DAR protection is required for the outer layer and the inner layer, provided through the SF, HF, or HS solution designs. When using the RM use case, choose from the SF, HF, or HS solution designs. Requirements of the SF, HF, or HS solution design should be followed with this use case. For example, if the HF solution design is chosen, both HF and RM requirements are applicable.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY

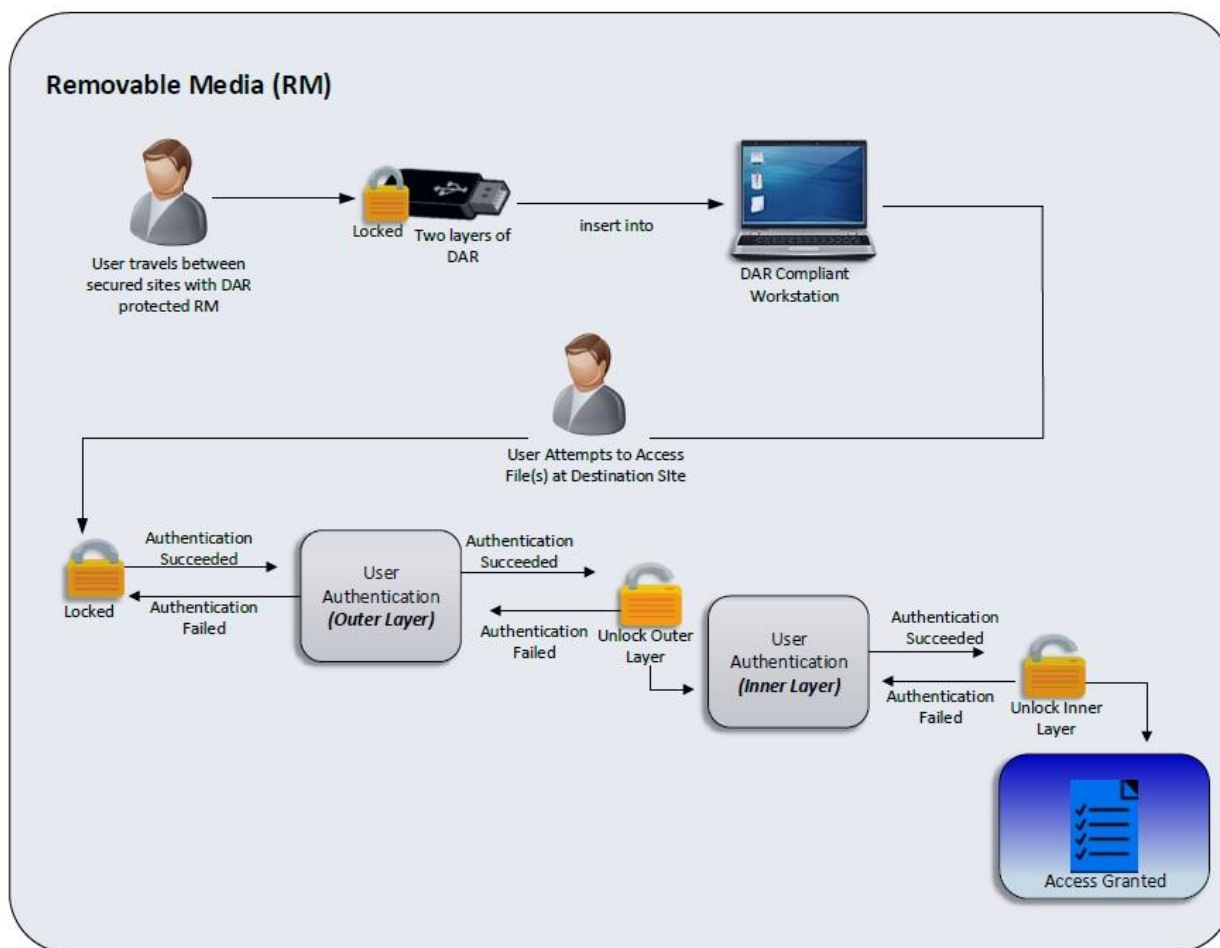


Figure 5: Removable Media Solution Design

The PF solution design cannot be employed on removable media because there are several incompatibilities between their requirements. The PE layer is used only as the outer layer and requires hardware-backed secure key storage, with the goal of reducing the need for long and complex passwords. Each layer of encryption in the PF DAR solution may use similar authentication mechanism types (e.g., passwords) but requires a unique authorization credential for each layer.

RM use case only protects endpoints as stated in this CP or in a secured facility. The LF use case is prohibited when using removable media for DAR protection. If the removable media is lost and out of continuous physical control, users shall report it to their Information Systems Security Officer (ISSO) or chain of command, as defined by the AO. The removable media is considered compromised once lost and cannot be re-used if later found. Lost and Found requirements do not guarantee or protect the integrity of the removable media once lost and out of continuous physical control.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



7 CONFIGURATION REQUIREMENTS

Sections 7 through 12 specify requirements for implementations of the four solutions compliant with this CP. The tables of requirements in the following sections have a column that specifies which solutions the requirement applies to, and uses the following nomenclature:

- SF design: DAR solution components include SWFDE and FE.
- PF design: DAR solution components include PE and FE.
- HF design: DAR solution components include HWFDE and FE.
- HS design: DAR solution components include HWFDE and SWFDE.
- RM design: DAR solution design include SF, HF, or HS components.

The CP includes two categories of requirements:

- An Objective (O) requirement specifies a feature or function that is desired or expected. Organizations should implement objective requirements in lieu of corresponding Threshold requirements where feasible.
- A Threshold (T) requirement specifies a minimum acceptable feature or function that still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to system maturity). A solution implementation must satisfy all applicable Threshold requirements, or their corresponding Objective requirements, in order to comply with this CP.

In many cases, the Threshold requirement also serves as the Objective requirement (T=O). In some cases, multiple versions of a requirement may exist in this CP. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement. Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement improves upon the Threshold requirement and may replace the Threshold requirement in future versions of this CP. Objective requirements without corresponding Threshold requirements are marked as “Optional”, but improve upon the overall security of the solution and should be implemented where feasible.

In order to comply with this CP, a solution must, at minimum, implement all Threshold requirements associated with each of the solution designs it supports and should implement the Objective requirements associated with those solution designs where feasible. For example, a DAR solution utilizing an SWFDE and FE must implement only those Threshold requirements applicable to the SF design.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



The customer may treat the device as being classified; however, if they do so, they must adhere to the policies and requirements for classified devices (note that those requirements exceed the requirements contained within the DAR CP).

Each requirement defined in this CP has a unique identifier digraph that groups related requirements together (e.g., KM), and a sequence number (e.g., 2). Table 3 lists the digraphs used to group together related requirements, and identifies where they can be found in the following sections.

Table 3: Requirement Digraphs

| Digraph | Description | Section(s) | Table(s) |
|---------|--|--------------|----------|
| PS | Product Selection Requirements | Section 8 | Table 4 |
| SR | Overall Solution Requirements | Section 9.1 | Table 5 |
| CR | Configuration Requirements for All DAR Components | Section 9.2 | Table 6 |
| SW | Requirements for SWFDE Components | Section 9.3 | Table 7 |
| FE | Requirements for FE Components | Section 9.4 | Table 8 |
| PE | Requirements for PE Components | Section 9.5 | Table 9 |
| HW | Requirements for HWFDE Components | Section 9.6 | Table 10 |
| EU | Requirements for EUD | Section 9.7 | Table 11 |
| CM | Configuration Change Detection Requirements | Section 9.8 | Table 12 |
| DM | Requirements for Device Management | Section 9.9 | Table 13 |
| AU | Auditing Requirements | Section 9.10 | Table 14 |
| KM | Key Management Requirements for All DAR Components | Section 9.11 | Table 15 |
| SC | Requirements for Supply Chain Risk Management | Section 9.12 | Table 16 |
| LF | Requirements for Lost and Found | Section 9.13 | Table 17 |
| GD | Requirements for Use and Handling of Solutions | Section 10.1 | Table 18 |
| RP | Requirements for Incident Reporting | Section 10.2 | Table 19 |
| TR | Testing Requirements | Section 12.1 | Table 20 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



8 REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are provided for maximizing the independence of components within the solution. This will increase the level of effort required to compromise this solution.

Table 4: Product Selection Requirements

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|-------------------------|-------------|
| DAR-PS-1 | The products used for the FE layer shall be chosen from the list of FE products on the CSfC Components List. | HF, SF, PF, RM | T=O | |
| DAR-PS-2 | The products used for the SWFDE layer shall be chosen from the list of SWFDEs on the CSfC Components List. | HS, SF, RM | T=O | |
| DAR-PS-3 | The Inner and Outer DAR layers shall either: <ul style="list-style-type: none">• Come from different manufacturers, where neither manufacturer is a subsidiary of the other; or• Be different products from the same manufacturer, where NSA has determined that the products meet the CSfC Program's criteria for implementation independence. | HF, HS, SF, PF, RM | T=O | |
| DAR-PS-4 | (Moved to DAR-SC-2) | | | |
| DAR-PS-5 | The cryptographic libraries used by the Inner and Outer DAR layers shall be independently developed and implemented. | HF, HS, SF, PF, RM | O | Optional |
| DAR-PS-6 | The products used for the PE layer shall be chosen from the list of PE products on the CSfC Components List under the Mobile Platform section. | PF | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|------------------|----------------------|-------------|
| DAR-PS-7 | The products used for the HWFDE layer shall be chosen from the list of HWFDEs on the CSfC Components List. | HF, HS, RM | T=O | |

9 CONFIGURATION

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components for a DAR solution.

9.1 OVERALL SOLUTION REQUIREMENTS

Table 5: Overall Solution Requirements

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|----------------------|-------------|
| DAR-SR-1 | Default accounts, passwords, community strings, and other default access control mechanisms for all components shall be changed or removed. | SF, PF, HF, HS, RM | T=O | |
| DAR-SR-2 | The DAR solution shall be properly configured according to local policy and U.S. Government guidance (e.g., NSA guidelines). In the event of conflict between the requirements in this CP and local policy, the CSfC Program Management Office (PMO) shall be contacted. | SF, PF, HF, HS, RM | T=O | |
| DAR-SR-3 | Each DAR component shall have a unique account for each user. | SF, PF, HF, HS | O | Optional |
| DAR-SR-4 | All EUDs shall remain in continuous physical control at all times, as defined by the AO. | HF, HS, SF, PF, RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | | | | |
|----------|--|--------------------|-----|----------|
| DAR-SR-5 | The AO shall provide guidance for when CE should be implemented. | HF, HS, PF, SF, RM | O | Optional |
| DAR-SR-6 | The AO shall provide procedures for performing CE. | HF, HS, PF, SF, RM | O | Optional |
| DAR-SR-7 | At least one layer shall use a trusted platform module for cryptographic key storage. | HF, HS, SF | O | Optional |
| DAR-SR-8 | If the Lost and Found use case is implemented, then the Lost and Found requirements (Table 17) shall be implemented. | SF, PF, HF, HS | T=O | |

9.2 CONFIGURATION REQUIREMENTS FOR ALL DAR COMPONENTS

Table 6: Configuration Requirements for All DAR Components

| Req # | Requirement Description | Solution Designs | Threshold/Objective | Alternative |
|----------|--|--------------------|---------------------|-------------|
| DAR-CR-1 | Default encryption keys shall be changed. | SF, PF, HF, HS, RM | T=O | |
| DAR-CR-2 | Primary user authentication credential values for each DAR layer mechanism type shall be unique (e.g., the password for the 1 st layer will not be the same as the password for the 2 nd layer). | SF, PF, HF, HS, RM | T=O | |
| DAR-CR-3 | DAR components shall use algorithms for encryption selected from Table 1 that are approved to protect the highest classification level of the data. | SF, PF, HF, HS, RM | T=O | |
| DAR-CR-4 | Each DAR component shall prevent further authentication attempts after a number of failed attempts defined by the AO. | SF, PF, HF, HS, RM | O | Optional |
| DAR-CR-5 | Each DAR layer shall perform a CE after a number of consecutive failed logon attempts as defined by the AO. | SF, PF, HF, HS, RM | O | Optional |
| DAR-CR-6 | Each DAR component shall locally generate its own symmetric encryption keys on the EUD. | SF, PF, HF, HS, RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|-----------|--|--------------------|----------------------|-------------|
| DAR-CR-7 | Each DAR component shall permit only an administrator to disable DAR component. | SF, HF, HS, PF, RM | O | Optional |
| DAR-CR-8 | All components shall have DAR protections enabled at all times after provisioning. | SF, PF, HF, HS, RM | T=O | |
| DAR-CR-9 | All components shall encrypt all classified data. (Refer to Section 5.2 for additional information on FE.) | SF, PF, HF, HS, RM | T=O | |
| DAR-CR-10 | All CSfC components shall be implemented (configured) using only their NIAP-approved configuration settings. User may change settings that are not part of NIAP evaluation. | SF, PF, HF, HS, RM | T=O | |
| DAR-CR-11 | Users shall be restricted to designated user folders. | SF, HF | T=O | |
| DAR-CR-12 | For use in high threat environments (as defined by the AO) the two layers of DAR shall use different primary authentication factors (e.g., Both layers cannot use passwords. One layer may use a password but the second layer would then need to use a token or other factor). | HF, HS, SF, RM | T=O | |
| DAR-CR-13 | For use in routine threat environments (as defined by the AO) the two layers of DAR shall use different primary authentication factors (e.g., Both layers cannot use passwords. One layer may use a password but the second layer would then need to use a token or other factor). | HF, HS, SF, RM | O | Optional |
| DAR-CR-14 | At least one DAR layer shall use multi-factor authentication. | HF, HS, SF, RM | O | Optional |
| DAR-CR-15 | The removable media shall not be bootable. | RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



9.3 REQUIREMENTS FOR SWFDE COMPONENTS

Table 7: Requirements for SWFDE Components

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|------------------|----------------------|-------------|
| DAR-SW-1 | The SWFDE shall use Cipher Block Chaining (CBC) for data encryption. | SF, HS, RM | T | DAR-SW-2 |
| DAR-SW-2 | The SWFDE shall use XTS or Galois/Counter Mode (GCM) for data encryption. | SF, HS, RM | O | DAR-SW-1 |
| DAR-SW-3 | The SWFDE shall be configured to use one of the following primary authentication options: <ul style="list-style-type: none">• A randomly generated passphrase that meets the minimum strength set in Appendix D. Password/Passphrase Strength Parameters or• A randomly generated password that meets the minimum strength set in Appendix D. Password/Passphrase Strength Parameters or• A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token or• Any combination of the above. | SF, HS, RM | T=O | |

9.4 REQUIREMENTS FOR FE COMPONENTS

Table 8: Requirements for FE Components

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|------------------|----------------------|-------------|
| DAR-FE-1 | The FE product shall use CBC for data encryption. | SF, PF, HF, RM | T | DAR-FE-2 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|------------------|----------------------|-------------|
| DAR-FE-2 | The FE product shall use XTS for data encryption. | SF, PF, HF, RM | O | DAR-FE-1 |
| DAR-FE-3 | The FE product shall use one of the following primary authentication options: <ul style="list-style-type: none">A randomly generated or user-generated passphrase or password defined by the AO that meets minimum strength set in Appendix D. Password/Passphrase Strength orAn external smartcard or software capability containing a software certificate with RSA or Elliptic Curve Cryptography (ECC) key pairs per Table 1. | SF, PF, HF, RM | T=O | |

9.5 REQUIREMENTS FOR PE COMPONENTS

Table 9: Requirements for PE Components

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|------------------|----------------------|-------------|
| DAR-PE-1 | The PE shall enable the “wipe sensitive data” management function for imported or self-generated keys/secrets and/or other classified data. | PF | T=O | |
| DAR-PE-2 | The PE shall use CBC for data encryption. | PF | T | DAR-PE-3 |
| DAR-PE-3 | The PE shall use XTS or Galois/Counter Mode (GCM) for data encryption. | PF | O | DAR-PE-2 |
| DAR-PE-4 | The AO shall provide policy to the user determining when data or keys must be wiped. | PF | T=O | |
| DAR-PE-5 | The PE product shall use one of the following primary authentication | PF | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|-------|--|------------------|----------------------|-------------|
| | options: A minimum of a six-character, case-sensitive alphanumeric password with the length and complexity as defined by the AO, or a passphrase with the length and complexity as defined by the AO. | | | |

9.6 REQUIREMENTS FOR HWFDE COMPONENTS

Table 10: Requirements for HWFDE Components

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|------------------|----------------------|-------------|
| DAR-HW-1 | The HWFDE shall use CBC for data encryption. | HF, HS, RM | T | DAR-HW-2 |
| DAR-HW-2 | The HWFDE shall use GCM or XTS for data encryption. | HF, HS, RM | O | DAR-HW-1 |
| DAR-HW-3 | The HWFDE shall be configured to use one of the following primary authentication options: <ul style="list-style-type: none">• A randomly generated passphrase or password that meets the minimum strength set in Appendix D. Password/Passphrase Strength Parameters or• A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token or• A combination of both of the above. | HF, HS, RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



9.7 REQUIREMENTS FOR END USER DEVICES

Table 11: Requirements for End User Devices

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|--------------------|----------------------|--|
| DAR-EU-1 | All EUD provisioning shall be performed through direct physical access. | SF, PF, HF, HS, RM | T=O | |
| DAR-EU-2 | If found after being lost, the EUD's non-volatile storage media shall be destroyed per NSA/CSS Storage Device Sanitization (NSA/CSS Policy Manual 9-12). (This does not preclude having the device forensically analyzed by the appropriate authority.) | SF, PF, HF, HS, RM | T=O | (DAR-LF-3 if LF use case is implemented) |
| DAR-EU-3 | EUDs shall implement the Basic Input/Output System (BIOS) security guidelines specified in NIST SP 800-147. | SF, PF, HF, HS | O | Optional |
| DAR-EU-4 | All users shall sign an organization-defined user agreement before being authorized to use an EUD. | SF, PF, HF, HS, RM | T=O | |
| DAR-EU-5 | All users shall receive an organization-developed training course for operating an EUD prior to use. | SF, PF, HF, HS, RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|--------------------|----------------------|-------------|
| DAR-EU-6 | At a minimum, the organization-defined user agreement shall include each of the following: Consent to monitoring <ul style="list-style-type: none">Operational Security (OPSEC) guidanceRequired physical protections to employ when operating and storing the EUDRestrictions for when, where, and under what conditions the EUD may be usedResponsibility for reporting security incidentsVerification of IA trainingVerification of appropriate clearanceJustification for AccessRequester information and organizationAccount Expiration DateUser ResponsibilitiesAn overview of what constitutes continuous physical control and the risks associated with using the EUD after it is lost | SF, PF, HF, HS, RM | T=O | |
| DAR-EU-7 | External USB tokens and smartcards, when used for authentication, shall be removed from the EUD upon or before shut down in accordance with AO policy. | SF, PF, HF, HS, RM | T=O | |
| DAR-EU-8 | AO shall provide guidance on storing and/or securing authentication factors. | SF, PF, HF, HS, RM | T=O | |
| DAR-EU-9 | The SA shall disable system power saving states on EUDs (i.e., sleep and hibernate). | SF, HF, HS | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|-----------|---|--------------------|----------------------|-------------|
| DAR-EU-10 | The EUD shall power off after a period of inactivity defined by the AO. | SF, HF, HS | T=O | |
| DAR-EU-11 | The EUDs shall be provisioned within a physical environment certified to protect the highest classification level of the data stored on the device. | SF, PF, HF, HS, RM | T=O | |
| DAR-EU-12 | The EUD shall only be re-provisioned to the same or higher classification level of the classified data per an AO approved process. | SF, PF, HF, HS, RM | T=O | |
| DAR-EU-13 | The EUD shall be reported as "lost" when out of continuous physical control as specified by the AO. Alternate requirement DAR-LF-2 can only be used if all LF requirements are implemented. | SF, PF, HF, HS, RM | T=O | |
| DAR-EU-14 | System folders shall have user write permissions disabled unless authorized by an administrator. | SF, HF | T=O | |
| DAR-EU-15 | The EUD shall be protected with anti-tamper measures. | SF, PF, HF, HS, RM | O | Optional |
| DAR-EU-16 | The device shall be rebooted before and after if the EUD is handled by an unauthorized party (e.g., customs). | HF, HS, PF, SF | T=O | |
| DAR-EU-17 | The absence of any expected authentication prompt(s) shall be reported as possible tampering to the AO. | HF, HS, PF, SF, RM | T=O | |
| DAR-EU-18 | When data is no longer needed, it shall be overwritten or erased by secure erase tool per AO guidance. (See section 4.10) | HF, HS, PF, SF, RM | O | Optional |
| DAR-EU-19 | The EUD, when not in use outside of a secured facility, shall be kept in an AO-approved locked container. | HF, HS, PF, SF, RM | O | Optional |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/Objective | Alternative |
|-----------|---|--------------------|---------------------|--|
| DAR-EU-20 | The BIOS/Unified Extensible Firmware Interface (UEFI) shall be configured to require a password before continuing the boot process. | HF, HS, SF | O | Optional |
| DAR-EU-21 | All DAR FDE components shall be cryptographically erased before being provisioned again. | HF, HS, SF, RM | T=O | |
| DAR-EU-22 | All DAR components shall be cryptographically erased before being provisioned again. | PF | O | Optional |
| DAR-EU-23 | System folders shall have user write permissions disabled unless authorized by an administrator. | PF | O | Optional |
| DAR-EU-24 | The EUD shall enable the BIOS/UEFI password. | HF, HS, SF | O | Optional (DAR-LF-6 if LF use case is implemented) |
| DAR-EU-25 | If the user suspects the EUD has been compromised, the EUD user shall obtain authorization from their AO prior to use. | HF, HS, PF, SF, RM | O | Optional (DAR-LF-11 if LF use case is implemented) |
| DAR-EU-26 | Each EUD shall be personalized by the end user. (This should not violate any other security features.) | HF, HS, PF, SF, RM | O | Optional (DAR-LF-12 if LF use case is implemented) |
| DAR-EU-27 | A removable media EUD shall not be used as a smart card/USB Authentication Token if it is also storing encrypted user data. | RM | T=O | |
| DAR-EU-28 | The device shall be removed from a host system before being handled by an unauthorized party (e.g., customs). | RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



9.8 CONFIGURATION CHANGE DETECTION REQUIREMENTS

Table 12: Configuration Change Detection Requirements

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|----------------------|-------------|
| DAR-CM-1 | A history of baseline configuration for all components shall be maintained by the SA. | SF, PF, HF, HS, RM | T=O | |
| DAR-CM-2 | An automated process shall ensure configuration changes are logged. | SF, PF, HF, HS, RM | O | Optional |
| DAR-CM-3 | Log messages generated for configuration changes shall include the specific changes made to the configuration. | SF, PF, HF, HS, RM | O | Optional |
| DAR-CM-4 | A history of baseline configuration for all components shall be available to the auditor. | SF, PF, HF, HS, RM | T=O | |
| DAR-CM-5 | Configuration change logs shall be kept for an AO defined period of time. | SF, PF, HF, HS, RM | T=O | |

9.9 REQUIREMENTS FOR DEVICE MANAGEMENT

Table 13: Requirements for Device Management

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|----------------------|-------------|
| DAR-DM-1 | EUDs shall be physically administered. | SF, PF, HF, HS, RM | T | DAR-DM-2 |
| DAR-DM-2 | EUDs shall be remotely administered using an NSA-approved DIT protection solution (e.g., NSA Certified Product or CSfC approved solution). | SF, PF, HF, HS | O | DAR-DM-1 |
| DAR-DM-3 | Administration workstations shall be dedicated for the purposes given in the CP. | SF, PF, HF, HS | T=O | |
| DAR-DM-4 | Administration workstations shall physically reside within a protected facility where CSfC solution(s) are managed. | SF, PF, HF, HS | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|----------------------|-------------|
| DAR-DM-5 | Administration workstations shall be physically separated from workstations used to manage non-CSfC solutions. | SF, PF, HF, HS | T=O | |
| DAR-DM-6 | Only authorized SAs (See Section 11) shall be allowed to administer the DAR Components. | SF, PF, HF, HS, RM | T=O | |

9.10 AUDITING REQUIREMENTS

Table 14: Auditing Requirements

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|--------------------|----------------------|-------------|
| DAR-AU-1 | EUDs shall be inspected for malicious physical changes in accordance with AO defined policy. | SF, PF, HF, HS, RM | T=O | DAR-LF-7 |
| DAR-AU-2 | The EUDs shall be configured to generate an audit record of the following events: <ul style="list-style-type: none">Start-up and shutdown of any platform audit functions.All administrative actions affecting the DAR encryption components.User authentication attempts and success/failure of the attempts.Software updates to the DAR encryption components. | SF, PF, HF, HS, RM | O | Optional |
| DAR-AU-3 | Auditors shall review audit logs for a time period as defined by the AO. | SF, PF, HF, HS, RM | T=O | |
| DAR-AU-4 | Auditors shall physically account for the EUDs after an AO-defined time period. | SF, PF, HF, HS, RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|----------------------|-------------|
| DAR-AU-5 | Administrators shall periodically compare solution component configurations to a trusted baseline configuration after an AO-defined time period. | SF, PF, HF, HS, RM | O | Optional |

9.11 KEY MANAGEMENT REQUIREMENTS

Table 15: Key Management Requirements for All DAR Components

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|--------------------|----------------------|-------------|
| DAR-KM-1 | The key sizes used for each layer shall be as specified in Table 1. | SF, PF, HF, HS, RM | T=O | |
| DAR-KM-2 | DAR solution products shall be initially keyed within a physical environment certified to protect the highest classification level of the DAR solution. | SF, PF, HF, HS, RM | T=O | |
| DAR-KM-3 | The DAR solution shall disable all key recovery mechanisms. | SF, PF, HF, HS, RM | T=O | |
| DAR-KM-4 | The algorithms used for each layer shall be as specified in Table 1. | SF, PF, HF, HS, RM | T=O | |

9.12 SUPPLY CHAIN RISK MANAGEMENT REQUIREMENTS

Table 16: Supply Chain Risk Management Requirements

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|--------------------|----------------------|-------------|
| DAR-SC-1 | CSfC Trusted Integrators shall be employed to architect, design, procure, integrate, test, document, field, and support the solution. | SF, PF, HF, HS, RM | O | Optional |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|----------------------|-------------|
| DAR-SC-2 | Each component selected from the CSfC Components List shall go through a Product SCRM Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO-approved Product SCRM process. (See CNSSD 505 SCRM for additional guidance.) | HF, HS, SF, PF, RM | T=O | |

9.13 LOST AND FOUND REQUIREMENTS

All of the following requirements must be met in order to implement the Lost and Found use case. The Lost and Found use case covers the scenario where an EUD has been recovered after having been out of continuous physical control (as defined by the AO) and the user wants to reuse the device. This is a high risk use case and requires a number of additional requirements to lower the risk.

Note that the Lost and Found use case is optional. If it is not implemented then the device cannot be reused if it is lost. The SF solution is not allowed for the Lost and Found use case. The LF use case is also prohibited when using removable media (RM) for DAR protection as explained in paragraph 6.5 above.

Table 17: Lost and Found Requirements

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|------------------|----------------------|-------------------|
| DAR-LF-1 | Organizational-developed training shall include guidance on tamper awareness and detection. | HF, HS, PF | T=O | |
| DAR-LF-2 | The EUD shall be reported as "compromised" when tampering, as defined by AO policy, is suspected. | HF, HS, PF | T=O | Replaces EU-13 |
| DAR-LF-3 | The EUD and/or non-volatile storage media, if found after compromise, shall be destroyed per NSA/CSS Storage Device Sanitization (NSA/CSS Policy Manual 9-12). (This does not preclude having the device forensically analyzed by the appropriate authority.) | HF, HS, PF | T=O | Replaces DAR-EU-2 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | | | | |
|-----------|--|------------|-----|--------------------|
| DAR-LF-4 | The two layers of DAR shall use different primary authentication factors (i.e., One layer may use a password but the second layer would need to use a token). | HF, HS | T=O | |
| DAR-LF-5 | EUDs shall use boot integrity verification technology. (see glossary) | HF, HS | T=O | |
| DAR-LF-6 | The EUD shall enable the BIOS/Unified Extensible Firmware Interface (UEFI) password. | HF, HS | T=O | Replaces DAR-EU-24 |
| DAR-LF-7 | Prior to reuse, the EUD shall undergo tamper detection inspection as established by the AO to determine if the device has been tampered with or substituted. | HF, HS, PF | T=O | |
| DAR-LF-8 | The EUD, when outside of a secured facility and not in use, shall be kept out of view. | HF, HS, PF | T=O | |
| DAR-LF-9 | If an unauthorized party takes the EUD out of sight or performs unknown operations the device shall be considered compromised. | HF, HS, PF | T=O | |
| DAR-LF-10 | When using commercial modes of travel (i.e., non-secure), the EUD shall stay with the traveler and not be placed in checked baggage. | HF, HS, PF | T=O | |
| DAR-LF-11 | If the user suspects the EUD has been compromised, the EUD user shall obtain authorization from the official appointed by the AO or local policy prior to use. | HF, HS, PF | T=O | Replaces DAR-EU-25 |
| DAR-LF-12 | Each EUD shall be personalized by the end user. (This should not violate any other security features.) | HF, HS, PF | T=O | Replaces DAR-EU-26 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



10 REQUIREMENTS SOLUTION OPERATION, MAINTENANCE, & HANDLING

10.1 REQUIREMENTS FOR THE USE AND HANDLING OF SOLUTIONS

The following requirements shall be followed regarding the use and handling of the solution.

Table 18: Requirements for the Use and Handling of Solutions

| Req # | Requirement Description | Solution Designs | Threshold/Objective | Alternative |
|----------|--|--------------------|---------------------|-------------|
| DAR-GD-1 | Acquisition and procurement documentation shall not include information about how the equipment will be used, including that it will be used to protect classified information. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-2 | The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure that it meets the latest version of the CP. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-3 | The AO will ensure that a compliance audit shall be conducted every year against the latest version of the DAR CP. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-4 | Results of the compliance audit shall be provided to and reviewed by the AO. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-5 | When a new, approved version of the DAR CP is published by NSA, the AO shall ensure compliance against this new CP within 6 months. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-6 | Solution implementation information, which was provided to NSA during solution registration, shall be updated every 12 (or fewer) months (see Section 12.3). | SF, PF, HF, HS, RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|-----------|---|--------------------|----------------------|-------------|
| DAR-GD-7 | The SA, auditor, user, and all Integrators shall be cleared to the highest level of data protected by the DAR solution. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-8 | The SA and auditor roles shall be performed by different people. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-9 | All SAs, users, and auditors shall meet local information assurance training requirements. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-10 | Users shall report lost or stolen EUDs to their ISSO or chain of command as defined by the AO. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-11 | Only SAs or CSfC Trusted Integrators shall perform the installation and policy configuration. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-12 | Security critical patches (such as Information Assurance Vulnerability Alert (IAVAs)) shall be tested and subsequently applied to all components in the solution in accordance with local policy and this CP. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-13 | Local policy shall dictate how the SA will install patches to solution components. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-14 | All DAR components shall be updated using digitally signed updates provided by the vendor. | SF, PF, HF, HS, RM | T=O | |
| DAR-GD-15 | All authorized users shall have the ability to CE keys for both layers. | SF, PF, HF, HS, RM | O | Optional |
| DAR-GD-16 | When using an FE Product, the user must ensure that no classified data shall be put into the file's metadata (e.g., filename). | SF, PF, HF, RM | T=O | |
| DAR-GD-17 | Withdrawn | | | |
| DAR-GD-18 | Withdrawn | | | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|-----------|--|--------------------|----------------------|-------------|
| DAR-GD-19 | AO shall define loss of continuous physical control for each use case. This definition shall cover the following topics: <ul style="list-style-type: none">• User handling• EUD Transportation• EUD Storage• Anti-tamper mechanisms and related policies, if any are used.• Device integrity measures and related policies, if any are used. | SF, PF, HF, HS, RM | T=O | |

10.2 REQUIREMENTS FOR INCIDENT REPORTING

Table 19 lists requirements to report security incidents to NSA regarding incidents affecting the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that SAs and auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for Operations and Maintenance (O&M) will be better equipped to identify reportable incidents.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary, but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

Table 19 only provides requirements directly related to the incident reporting process. See Section 9.10 for requirements supporting detection of events that may reveal that a reportable incident has occurred.

Table 19: Incident Reporting Requirements

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|---|--------------------|----------------------|-------------|
| DAR-RP-1 | Report a security failure in any of the CSfC DAR solution components. | SF, PF, HF, HS, RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|----------------------|-------------|
| DAR-RP-2 | Report any malicious configuration changes to the DAR components. | SF, PF, HF, HS, RM | T=O | |
| DAR-RP-3 | Report any evidence of a compromise of classified data caused by a failure of the CSfC DAR solution. Compromise, in this context, includes reporting real or perceived access to classified data (e.g., user or administrator access that occurs without proper authentication or through the use of incorrect credentials). | SF, PF, HF, HS, RM | T=O | |
| DAR-RP-4 | Report any evidence of malicious physical tampering (e.g., missing or mis-installed parts) with solution components. | SF, PF, HF, HS, RM | T=O | |
| DAR-RP-5 | Confirmed incidents meeting the criteria in DAR-RP-1 through DAR-RP-4 shall be reported within 24 hours of detection via Joint Incident Management System (JIMS) or contacting NSA as specified in the CSfC Registration Letter. | SF, PF, HF, HS, RM | T=O | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|----------------------|-------------|
| DAR-RP-6 | <p>At a minimum, the organization shall provide the following information when reporting security incidents:</p> <ul style="list-style-type: none">• CSfC Registration Number• Point of Contact (POC) name, phone, email• Alternate POC name, phone, email• Classification level of affected solution• Affected component(s) manufacturer/vendor• Affected component(s) model number• Affected component(s) version number• Date and time of incident• Description of incident• Description of remediation activities• Is Technical Support from NSA requested? (Yes/No) | SF, PF, HF, HS, RM | T=O | |

11 ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are detailed below, along with doctrinal requirements for these roles.

End User – An end user may operate an EUD from physical locations not owned, operated, or controlled by the Government. The end user shall be responsible for operating the EUD in accordance with this CP and an organization-defined user agreement. End user duties include, but are not limited to the following:

1. Ensuring that the EUD is only operated in physical spaces that comply with the end user agreement.
2. Alerting the Security Administrator immediately upon an EUD being lost, stolen, or suspected of being tampered with.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



Security Administrator – The SA shall be responsible for maintaining, monitoring, and controlling all security functions for the entire suite of products composing the DAR solution. Security Administrator duties include, but are not limited to the following:

1. Ensuring that the latest security critical software patches and updates (such as IAVAs) are applied to each product in a timely fashion.
2. Documenting and reporting security-related incidents to the appropriate authorities.
3. Coordinating and supporting product logistic support activities including integration and maintenance. Ensuring that the implemented DAR solution remains compliant with the latest version of the CP.
4. Provisioning and maintaining EUDs in accordance with this CP.

Auditor - The auditor shall be responsible for reviewing the actions performed by the SA and events recorded in the audit logs to ensure that no action or event represents a compromise of the DAR solution. The role of auditor and SA shall not be performed by the same individual. Auditor duties include but are not limited to the following:

1. Reviewing, managing, controlling, and maintaining security audit log data.
2. Documenting and reporting security-related incidents to the appropriate authorities.
3. The auditor will be given authority to access all audit records.

Integrator – Integrator duties may include but are not limited to the following:

1. Acquiring the products that compose the solution.
2. Configuring the DAR solution in accordance with the CP.
3. Testing the DAR solution.
4. Documenting the solution and its compliance to the CP.
5. Troubleshooting the solution.

In certain cases, an external integrator may be used to implement a DAR solution based on the CP. A CSfC Trusted Integrator is one such entity. The use of CSfC Trusted Integrators although not required, is highly recommended. A CSfC Trusted Integrator is defined as a selected organization that has demonstrated competency in:

1. System integration.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



2. The technologies to be integrated.
3. Formal testing processes.
4. Generating evidence for system authorization.

Chosen CSfC Trusted Integrator applicants are required to sign a Memorandum of Agreement (MoA) with NSA.

12 INFORMATION TO SUPPORT THE AO

This section details items that likely will be necessary for the customer to obtain approval from the system AO. The customer and AO have obligations to perform the following:

- The customer, possibly with support from an Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a test plan and perform testing of the DAR solution, see Section 12.1.
- The customer has system assessment and authorization performed using the risk assessment (RA) information referenced in Section 12.2.
- The customer provides the results from testing and from system assessment and authorization to the AO for use in making an approval decision. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented. NSA publishes compliance matrixes requiring a short description of how requirements are met. NSA recommends that the AO require the compliance matrix as part of their body of evidence.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 12.3. NSA publishes registration forms at <http://www.nsa.gov>.
- Customers who want to use a variant of the solution detailed in this CP will contact NSA early in their design phase to determine ways to obtain NSA approval.
- The AO will ensure that a compliance audit shall be conducted every year against the latest version of the DAR CP, and the results shall be provided to the AO.

12.1 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a DAR solution. This T&E will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this CP.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general, high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the DAR solution. The entire solution, to include each component described in Section 4.10, is addressed by this test plan.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



1. Set up the baseline network design and configure all components.
2. Document the baseline network design configuration. Include product model and serial numbers, and software version numbers as a minimum.
3. Develop a test plan for the specific implementation using the test objectives from Section 13. Any additional requirements imposed by the local AO should also be tested, and the test plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.
4. Perform testing using the test plan derived in Step 3. System testing will consist of both black box testing and gray box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.
5. Compile findings, including comments and vulnerability details as well as possible countermeasure information, into a final test report to be delivered to the AO for approval of the solution.
6. The following testing requirement has been developed to ensure that the DAR solution functions properly and meets the configuration requirements from Section 8. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 20: Test Requirements

| Req # | Requirement Description | Solution Designs | Threshold/ Objective | Alternative |
|----------|--|--------------------|----------------------|-------------|
| DAR-TR-1 | The organization implementing the CP shall perform all tests listed in Section 13. | HF, HS, PF, SF, RM | T=O | |

12.2 RISK ASSESSMENT

The RA of the DAR solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IA Customer Advocate to request the RA, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the RA is available on the SIPRNet CSfC website. The AO shall be provided a copy of the NSA RA for their consideration in approving the use of the solution.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



12.3 REGISTRATION OF SOLUTIONS

All customers using CSfC solutions to protect information on NSS shall register their solution with NSA prior to operational use. Customers will provide their compliance checklists and registration forms to NSA. This registration will allow NSA to track where DAR CP solutions are instantiated and to provide AOs at those sites with appropriate information, including all significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process, as well as the compliance matrices and registration forms, are available at http://www.nsa.gov/ia/programs/csfc_program.

Solution registrations are valid for one year, at which time customers are required to re-register their solution in order to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When a new version of this CP that has been approved by the IA Director is published, customers will have six months to bring their solutions into compliance with the new version and re-register them (see requirement DAR-GD-5). Customers are also required to update their registrations whenever the information provided on the registration form changes.

13 TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or Integrator to ensure they have properly configured the solution. As defined in Section 7, in order to comply with this CP, a solution must, at a minimum, implement all Threshold requirements associated with each of the capabilities it supports, and should implement the Objective requirements associated with those capabilities where feasible. These tests may also be used to provide evidence to the AO regarding compliance of the solution within this CP. Note that the details of the procedures are the responsibility of the final developer of the test plan in accordance with AO-approved network procedures. The AO is ultimately responsible for ensuring that all requirements from the CP have been properly implemented.

13.1 COMPONENT SELECTION

This section contains a procedure to verify that all components were selected to ensure independence in several important features.

Requirements being tested: DAR-PS-1 through DAR-PS-3, DAR-PS-5 through DAR-PS-7 and DAR-SC-2.

Procedure Description:

1. For each DAR layer, perform the following:
 - a. Verify that the FE is on the list of FEs on the CSfC Components List. (DAR-PS-1)
 - b. Verify that the SWFDE is on the list of SWFDEs on the CSfC Components List. (DAR-PS-2)



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



- c. Verify the products used for the PE layer are on the list of PE products on the CSfC Components List. (DAR-PS-6)
- d. Verify the products used for the HWFDE layer are on the list of HWFDEs on the CSfC Components List (DAR-PS-7)
- e. Verify that the two layers either come from different independent manufacturers or that NSA has determined that sufficient implementation independence exists. (DAR-PS-3)
- f. Verify that the cryptographic libraries used by the Inner and Outer DAR layers shall be independently developed and implemented (DAR-PS-5)
- g. Verify that each component selected from the CSfC Components List goes through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO approved Product Supply Chain Threat Assessment process. (See CNSSD 505 SCRM for additional guidance.) (DAR-SC-2)

Expected Results:

The results of the inspection should reveal that the DAR Solution components conform to the DAR CP.

13.2 END USER DEVICE CONFIGURATIONS

This section contains procedures to ensure that the configurations for all the EUDs in the DAR solution follow the requirements in this CP.

Requirements being tested: DAR-CR-12 through DAR-CR-14, DAR-EU-1, DAR-EU-3, DAR-EU-7 through DAR-EU-13, DAR-EU-15 through DAR-EU-22, DAR-EU-24, DAR-EU-25, DAR-SR-3, DAR-DM-1 through DAR-DM-6, DAR-LF-2, DAR-LF-5, DAR-LF-6 and DAR-LF-11.

Procedure Description:

1. For each EUD, perform the following:
 - a. Ensure that the implementing organization policy states that provisioning the EUD takes place in a facility that is at least equal to the highest classification level DAR solution and done through direct physical access. (DAR-EU-1 and DAR-EU-11)
 - b. Inspect the EUD to ensure passive anti-tamper measures are in place for each EUD. (DAR-EU-15)
 - c. Inspect the EUD's BIOS in order to verify that the BIOS complies with the security guidelines found in NIST-SP 800-147. (DAR-EU-3)



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



- d. Inspect the EUD to verify that boot integrity verification technology is enforced. (DAR-LF-5)
 - e. Inspect the EUD to ensure the BIOS/UEFI password is enabled. (DAR-LF-6, DAR-EU-24)
 - f. If applicable, ensure the BIOS is configured to require a password before continuing the boot process. (DAR-EU-20)
 - g. Ensure that all system power states on EUDs are disabled by the SA (i.e., sleep and hibernate). (DAR-EU-9)
 - h. Ensure the EUD is configured to shut down after a period of inactivity defined by the AO and does so. (DAR-EU-10)
 - i. Ensure the EUD is only re-provisioned to the same or higher classification level of the classified data per an AO-approved process. (DAR-EU-12)
 - j. Ensure all components are cryptographically erased before being provisioned again. (DAR-EU-21,22)
 - k. Verify an authorized secure erase tool is utilized to overwrite data that is no longer needed. (DAR-EU-18)
 - l. Verify that the implementing organization policy states that an EUD is considered and shall be reported as “lost” if out of continuous physical control as specified by the AO. (DAR-EU-13) or “compromised”. (DAR-LF-2)
 - m. Verify that the implementing organization policy states that if the user suspects that the EUD has been compromised that AO authorization to use is mandatory prior to use. (DAR-EU-25, DAR-LF-11)
 - n. Verify that the EUD has unique user accounts for each user. (DAR-SR-3)
 - o. Ensure that only authorized security administrators are allowed to administer the DAR components. (DAR-DM-6)
 - p. Ensure that EUDs are physically administered and that procedures are in place to perform this. (DAR-DM-1)
 - q. Ensure that EUDs are remotely administered using an NSA-approved DIT protection solution (e.g., NSA Certified Product or CSfC approved solution). (DAR-DM-2)
 - r. Ensure that Administration Workstations are dedicated and physically separated from workstations used to manage non-CSfC solutions. (DAR-DM-3, DAR-DM-5)
 - s. Ensure that Administration Workstations physically reside within a protected facility where CSfC solution(s) are managed. (DAR-DM-4)
2. If the EUD requires any external authentication factors, perform the following:
- a. Ensure the implementing organization policy states that USB tokens and Smartcards, when used, shall be removed from the EUD upon or before shut down in accordance with AO policy. (DAR-EU-7)
 - b. Ensure that the AO provides guidance on storing and securing authentication factors. (DAR-EU-8)



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



- c. Ensure the absence of any expected authentication prompts are reported as possible tampering to the AO. (DAR-EU-17)
3. If the EUD is to be used outside of a secured facility:
 - a. Ensure that the two layers of DAR are using different authentication methods. (DAR-CR-12, DAR-CR-13)
 - b. Alternatively, ensure at least one DAR layer uses multi-factor authentication. (DAR-CR-14)
 - c. Ensure an AO approved locked container is provided for the storage of the EUD when not in use outside of a secured facility. (DAR-EU-19)
 - d. Ensure the EUD is rebooted before and after being handled by an unauthorized party. (e.g., customs) (DAR-EU-16)

Expected Results:

For Step 1, all EUDs should be configured properly. For Step 2, an EUD utilizing a token should follow organizational policy for handling and storing authentication factors. For Step 3, the EUD should provide for different or multiple authentication factors or storage containers.

13.3 DAR COMPONENT CONFIGURATION

This section contains procedures to ensure that the configurations for all the DAR Components in the DAR solution follow requirements given in this CP.

Requirements being tested: DAR-SR-1, DAR-SR-2, DAR-SR-7, DAR-CR-1 through DAR-CR-11, DAR-EU-14, DAR-EU-23, DAR-SW-1 through DAR-SW-3, DAR-FE-1, DAR-FE-2, DAR-HW-1 through DAR-HW-3, DAR-GD-15, DAR-KM-1, DAR-KM-3 and DAR-KM-4, DAR-PE-1 through DAR-PE-5.

Procedure Description:

1. For each DAR component in the solution, perform the following:
 - a. Obtain the current configuration for the DAR Component.
 - b. Verify that all default accounts, passwords, community strings, and other default access control mechanisms are changed or removed. (DAR-SR-1)
 - c. Verify that the component is configured according to local policy and U.S. Government guidance (e.g., NSA Guidelines). In the event of conflict between the requirements in this CP and local policy, the CSfC PMO must be contacted. (DAR-SR-2)
 - d. Review documentation to verify all default encryption keys have been changed before the component is used. (DAR-CR-1)



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



- e. Verify that the user authentication credentials for each DAR layer mechanism type are unique. (DAR-CR-2)
 - f. Ensure that DAR components use algorithms for encryption selected from Table 1, which are approved to protect the highest classification level of the data. (DAR-CR-3)
 - g. Enter the number of failed attempts as defined by the AO to ensure that the user is locked out and is not allowed any further authentication attempts. (DAR-CR-4)
 - h. Enter the number of wrong passwords consecutively as defined by the AO and verify that the Data Encryption Key (DEK) is cryptographically erased by each DAR layer. (DAR-CR-5)
 - i. Ensure each DAR component generates its own symmetric encryption keys. (DAR-CR-6)
 - j. Ensure that each DAR component is configured to enable only an administrator to disable DAR component. (DAR-CR-7)
 - k. Ensure that all components have DAR protections enabled at all times after provisioning. (DAR-CR-8)
 - l. Ensure that all components encrypt all classified data. (DAR-CR-9)
 - m. Ensure that all CSfC components are implemented (configured) using only their NIAP-approved configuration settings. (DAR-CR-10)
 - n. Ensure that all key sizes used for the DAR components use the algorithms as specified in Table 1. (DAR-KM-1)
 - o. Verify that all key recovery mechanisms are disabled. (DAR-KM-3)
 - p. Ensure that all algorithms used for the DAR components use the algorithms as specified in Table 1. (DAR-KM-4)
2. For each SWFDE component in the solution, perform the following:
- a. Verify the SWFDE uses CBC, GCM, or XEX-based tweaked-codebook mode with cipher text stealing (XTS) for encryption. (DAR-SW-1, DAR-SW-2)
 - b. Verify that SWFDE is configured to use one of the following authentication options (DAR-SW-3):



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



- i. A randomly generated passphrase or password that meets the minimum strength set in Appendix D. Password/Passphrase Strength Parameters.
 - ii. A randomly-generated bit string equivalent to the crypto variable strength of the DEK contained on an external USB token.
 - iii. A combination of both of the above.
3. For each FE component in the solution, perform the following:
 - a. Verify that user write permissions to system folders are disabled unless authorized by an administrator. (DAR-EU-14, DAR-EU-23)
 - b. Verify that only CBC or XTS are utilized for encryption. (DAR-FE-1)
 - c. Ensure that the cryptographic erasure of all cryptographic keys is enabled per AO guidelines. (DAR-GD-15)
 - d. Verify that each user is restricted to their designated user folder. (DAR-CR-11)
 - e. Verify that the FE uses one of the following authentication options (DAR-FE-2):
 - i. A passphrase or password with the length and complexity defined in Appendix D. Password/Passphrase Strength Parameters.
 - ii. An external smartcard or software capability containing a software certificate with RSA or ECC key pairs.
4. For each PE component in the solution, perform the following:
 - a. Verify that the “wipe sensitive data” function is enabled for imported or self-generated keys/secrets and/or other classified data. (DAR-PE-1)
 - b. Verify that the encryption algorithms being used are CBC, GCM or XTS. (DAR-PE-2 and/or DAR-PE-3)
 - c. Ensure that the implementing organization AO provides policy to the user determining when data and/or keys need to be wiped. (DAR-PE-4)
 - d. Verify that PE component accepts a password, passphrase, or pin with the length and complexity defined by the AO. (DAR-PE-5)
5. For each HWFDE component in the solution, perform the following:



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



- a. Verify that the encryption algorithms being used are CBC or XTS. (DAR-HW-1 and/or DAR-HW-2)
- b. Verify that HWFDE is configured to use one of the following authentication options (DAR-HW-3):
 - i. A randomly generated passphrase or password that meets the minimum strength set in Appendix D. Password/Passphrase Strength Parameters.
 - ii. A randomly-generated bit string equivalent to the crypto variable strength of the DEK contained on an external USB token.
 - iii. A combination of the above.
6. If applicable, verify at least one layer uses a trusted platform module for cryptographic key storage. (DAR-SR-7)

Expected Results:

For Step 1, verify that all DAR components are properly configured and operating correctly. For Step 2, verify that the SWFDE DAR component is properly configured and operating correctly. For Step 3, verify that the FE DAR component is properly configured and operating correctly. For Step 4, verify that all PE DAR components within this solution are properly configured and operating correctly. For Step 5, verify that all HWFDE DAR components are properly configured and operating correctly. For Step 6, verify that there is at least one layer using a trusted platform module for cryptographic key storage.

13.4 CONFIGURATION CHANGE DETECTION

This section contains procedures to ensure that changes made to any of the DAR Component configurations are detected by the Configuration Change Detection tool.

Requirements being tested: DAR-CM-1 through DAR-CM-5, DAR-AU-5.

Procedure Description:

1. The following steps shall be performed for each of the DAR Components within the solution.
 - a. Ensure that a history of the baseline configuration for all components is maintained by the Security Administrator and is made available to the Auditor. (DAR-CM-1, DAR-CM-4)
 - b. Verify that procedures are in place for administrators to periodically compare solution component configurations to a trusted baseline configuration after an AO-defined time period. (DAR-AU-5)
 - c. Ensure that an automated process is enabled to log all configuration changes. (DAR-CM-2)



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



- d. Make a configuration change. Look in the audit log to verify that a log entry has been generated about the configuration change and that the specific changes are properly recorded. Do this several times with different types of changes, and then return to the initial configuration to complete. (DAR-CM-3)
- e. Ensure that a baseline configuration for all components is maintained by the Security Administrator and is retained for the time period as specified by the AO. (DAR-CM-4)
- f. Ensure that configuration change logs are maintained by the Security Administrator and stored for the period of time defined by the AO defined. (DAR-CM-5)

Expected Results:

The Auditor will validate the baseline configuration was stored in Step 1a. In Step 1d, there should be a log entry created for each configuration change in the audit log including the actual configuration change.

13.5 AUDIT

This section contains procedures for ensuring audit events are detected; the proper information is logged for each event.

Requirements being tested: DAR-AU-1 through DAR-AU-4.

Procedure Description:

1. Verify that EUDs are inspected for malicious physical changes in accordance with AO defined policy. (DAR-AU-1)
2. Examples for testing the ability of each DAR Component to audit and log audit events specified in the CP are given below. Verify that for each event logged, the applicable data regarding the event is recorded for the log entry. (DAR-AU-2)
 - a. Start up and shut down the EUD and any platforms therein that operate independently. Review the audit logs to verify that the start-up and shutdown events are recorded.
 - b. Verify that any actions taken as an administrator affecting the DAR encryption components are logged.
 - c. Authenticate to both layers on the EUD successfully. Then logout and attempt to re-authenticate to both layers but purposely enter the wrong authentication credentials. Review the audit logs to verify the success/failure of authentication attempts.
 - d. Send software updates to the DAR encryption components to verify that the updates are recorded in the audit log.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



3. Inspect the organization's implementation policy to verify that it states how often audit logs shall be reviewed by the Auditor per an AO defined time period. (DAR-AU-3)
4. Inspect the organization's implementing policy to verify how often the Auditor shall physically account for all EUDs in the DAR solution per an AO-defined time period. (DAR-AU-4)

Expected Results:

For Step 1, a procedure is in place to inspect EUDs for malicious physical changes. For Step 2, all occurrences of auditable events given should generate an entry in the audit log. For Steps 3 and 4, ensure that the implementing organization has a policy that complies with those requirements.

13.6 KEY MANAGEMENT

This section contains procedures to ensure that the generation and management of keys used in the DAR solution follow the requirements given in this CP.

Requirements being tested: DAR-KM-2.

Procedure Description:

1. Verify that the DAR Components are initially keyed within a physical environment certified to protect the highest classification level of the DAR solution. (DAR-KM-2)

Expected Results:

All DAR Components should be keyed properly according to the requirements found in this CP.

13.7 IMPLEMENTATION OF GUIDANCE

This section ensures that there are procedures in place and/or that procedures were followed regarding the procurement of products and use of the DAR solution. It also ensures the personnel are in place to manage and administer this solution following the guidelines given in the CP.

Requirements being tested: DAR-GD-1 through DAR-GD-16, DAR-GD-19, DAR-EU-2, DAR-EU-4 through DAR-EU-6, DAR-EU-26, DAR-EU-27, DAR-SR-4 through DAR-SR-6, DAR-SR-8, DAR-LF-1 through DAR-LF-4, DAR-LF-7 through DAR-LF-12 and DAR-SC-1.

Procedure Description:

1. Verify that the use and handling requirements given in DAR-GD-1 through DAR-GD-4, DAR-GD-7 through DAR-GD-16, DAR-GD-19, DAR-EU-2, DAR-EU-26, DAR-EU-27, DAR-LF-2 through DAR-LF-4 and DAR-LF-7 through DAR-LF-12 are currently in place and known to the users. (DAR-GD-1 through DAR-GD-4, DAR-GD-7 through DAR-GD-16, DAR-GD-19, DAR-EU-2, DAR-EU-26, DAR-EU-27, DAR-LF-2 through DAR-LF-4, and DAR-LF-7 through DAR-LF-12)



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



2. Verify that if the Lost and Found use case has been implemented that the Lost and Found requirements contained in Table 17 are implemented. (DAR-SR-8)
3. Verify that the AO guidance and procedures for when cryptographic erase should be implemented have been provided. (DAR-SR-5, DAR-SR-6)
4. Ensure that the implementing organization policy states that all users are required to sign an organization-defined user agreement before being authorized to use an EUD. (DAR-EU-4)
5. Verify that the implementing organization has a training program in place for users to receive prior to operating an EUD. (DAR-EU-5 and DAR-SR-4)
6. Verify that, at a minimum, the organization-defined user agreement includes each of the following (DAR-EU-6):
 - a. Consent to monitoring
 - b. OPSEC guidance
 - c. Required physical protections to employ when operating and storing the EUD
 - d. Restrictions for when and where the EUD may be used
 - e. Responsibility for reporting security incidents
 - f. Verification of IA Training
 - g. Verification of appropriate clearance
 - h. Justification for access
 - i. Requester information and organization
 - j. Account expiration date
 - k. User responsibilities
 - l. An overview of what constitutes continuous physical control and the risks associated with using the EUD after it is lost
7. Verify that Organizational-developed training includes guidance on tamper-awareness and detection. (DAR-LF-1)



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



8. Verify whether or not CSfC Trusted Integrators were employed to architect, design, integrate, test, document, field, and support solution. (DAR-SC-1)
9. Verify the solution owner and AO are aware that when new versions of the DAR CP are published by NSA, the AO shall ensure compliance against this new CP within 6 months. (DAR-GD-5)
10. Verify the solution owner and the AO are aware they shall provide updated solution information on a yearly basis. (DAR-GD-6)

Expected Results:

For Steps 1 and 2, all of these procedures have been followed or are in place. For Steps 3-5, the users are aware of their roles and responsibilities with respect to the use of the EUD. For Step 6, confirming whether or not CSfC Trusted Integrators were employed as appropriate.

13.8 INCIDENT REPORTING GUIDANCE

This section ensures that procedures are followed regarding incident reporting to NSA in the event a solution owner identifies a security incident which affects the solution.

Requirements being tested: DAR-RP-1 through DAR-RP-6.

Procedure Description:

1. Verify that the requirements for reporting security incidents to NSA given in DAR-RP-1 through DAR-RP-6 are currently in place and known to the users. (DAR-RP-1 through DAR-RP-6)

Expected Results:

For Step 1, all of these procedures have been followed or are in place.

13.9 SOLUTION FUNCTIONALITY

This section contains a procedure for ensuring the implementing organization complies with the testing requirements.

Requirements being tested: DAR-TR-1.

Procedure Description:

1. The implementing organization's AO will inspect the test report in order to ensure all testing requirements have been met (DAR-TR-1).

Expected Results:

The report will ensure that the implementing organization complies with the testing requirements.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



APPENDIX A. GLOSSARY OF TERMS

Administration Workstation - This device is commonly used for logging, configuration review, and management of the EUD.

Assessment - The technical evaluation of a system's security features performed as part of, and in support of, the approval/accreditation process that establishes the extent to which a particular computer systems design and implementation meet a set of specified security requirements.

Assessment and Authorization - A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37)

Assurance - A measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

Audit - The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rogue behavior.

Authentication - The process of confirming the identity of a user.

Authorization - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls (NIST 800-37). It can also be the decision to allow or deny a subject access to an object. For example, after a user has been authenticated, authorization determines if the user has the rights to perform specific actions on the device.

Boot Integrity Verification - These features ensure no code is executed during the boot process that has not first been verified for its integrity and authenticity. Each step in the boot process should verify the integrity of the next piece of code to execute before handing execution over to it. In current PC technology, this operates in two stages. First, the integrity and authenticity of the firmware is verified using a platform/vendor specific technology. Second, UEFI secure boot verifies the option ROMs and the OS loader before execution is handed over to the operating system.

Capability Package (CP) - The set of guidance provided by NSA that describes recommended approaches to provide architectures and configuration requirements that empower IA customers to implement



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



secure solutions using independent, layered COTS components to protect classified information. This package will point to potential products that can be used as part of this solution. The CPs are product-neutral and describe system-level solution frameworks documenting security and configuration requirements for customers and Integrators.

Commercial National Security Algorithm (CNSA) - Set of commercial algorithms capable of protecting data through Top Secret level (previously known as Suite B).

Committee on National Security Systems Policy No. 15 (CNSSP-15) - Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Compromise - Any computing resource whose confidentiality, integrity, or availability has been adversely impacted, either intentionally or unintentionally.

Cryptographic Erase - The process of sanitizing all data on a device.

DAR Component - Consists of a component that is part of the DAR solution (e.g., HWFDE, SWFDE, PE).

DAR Solution - A DAR Solution consists of two layered components (e.g., HWFDE and SWFDE).

Designated Approving Authority (DAA) - The official with the authority to formally assume responsibility for opening a system at an acceptable level of risk, synonymous with designating accrediting authority and delegated accrediting authority. (CNSSI 4009)

End User Device (EUD) - Any computing or storage device that can store data on it when it is powered off (in the context of this DAR document).

False Acceptance – when a different user will pass the biometric when they should not

False Rejection – when an authorized user's measurements fail to authenticate

Federal Information Processing Standards (FIPS) - A set of standards that describes the handling and processing of information within governmental agencies.

File Encryption (FE) - File encryption is the process of encrypting individual files or sets of files on an EUD and permitting access to the encrypted data only after proper authentication is provided.

Found Device - A lost device that has been recovered. (See Lost Device definition.)

Full Disk Encryption (FDE) - Also known as whole disk encryption, is the process of encrypting all the data on the drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the FDE product.

HF - DAR solution architecture that features an HWFDE layer under the FE layer.

HS - DAR solution architecture that features an HWFDE layer under the SWFDE layer.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



IA-Enabled Information Technology Product - Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security enabled messaging systems.

IA-enabled product - Product whose primary role is not security, but provides security services as an associated feature of its intended operating capabilities.

IA Product - Product whose primary purpose is to provide security services (e.g. confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks.

ISV - An independent software vendor (ISV) is a separate vendor that provides a product for managing a self-encrypting drive and provides a user interface to the drive.

Known Secret - PIN, password, or passphrase.

Layer - Every DAR solution protects classified data with two layers (e.g., HWFDE, SWFDE, FE, and PE).

Lost Device - A device that is removed from the control of the physical security procedures defined by the AO.

Network Attached Storage (NAS) - A file-level computer data storage server connected to a computer network providing data access to a group of clients. A NAS is a specialized computer built for storing and serving files.

Passive Anti-Tamper Measures - These measures serve to deter or delay modification of an EUD. They also aid in detecting attempts to modify the EUD or inject a substitute device. Examples include personalization options such as stickers, screen savers, wall papers, or other personalization methods which do not interfere with the configuration of the device.

PF - DAR solution architecture that features a PE layer under the FE layer.

Platform Encryption (PE) - A device that has met the requirements (and high assurance use case) of the Mobile Device Fundamentals Protection Profile (MDF PP).

Continuous Physical Control - The AO defines what is considered "Continuous Physical Control".

Pre-Boot Environment (PBE) - The initial software that is executed on start-up of the EUD that requires a user to authenticate successfully before decrypting and booting an operating system. This is the layer of authentication for the SWFDE product.

Protection Profile (PP) - A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information Assurance security requirements.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



Removable Media (RM) – A device which has the primary purpose of providing external storage of data protected by DAR through implementing two layers of encryption.

Rooted - The process of modifying a device such that it allows users to attain administrative privileges (i.e., root access).

Salt - A salt is random data that is added to a one-way function which hashes a password or passphrase in order to defeat dictionary attacks and pre-computed rainbow tables.

Secure Erase - The process of removing of all keys from a device in order to make decryption of data infeasible.

SF - DAR solution architecture that features an SWFDE layer under the FE layer.

Software Full Disk Encryption (SWFDE) - A software product that provides Full Disk Encryption.

Storage Area Network (SAN) - A dedicated network that provides access to consolidated, block level data storage. SANs devices appear like locally attached devices to the client operating system.

Supply Chain Risk Management (SCRM) - A program to establish processes and procedures to minimize acquisition-related risks to critical acquisitions including, hardware components and software solutions from supply chain threats due to reliance on global sources of supply.

Unauthenticated State - The state an EUD is in when the identity of a user, user device, or other entity has not been verified.

Volume - a collection of separate units of logically divided media (partition) acting as a single entity that has been formatted with a file system.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



APPENDIX B. ACRONYMS

| Acronym | Definition |
|---------|--|
| AES | Advanced Encryption Standard |
| AK | Authentication Key |
| AO | Authorizing Official |
| ASPP | Application Software Protection Profile |
| BIOS | Basic Input/Output System |
| CA | Client Advocate |
| CBC | Cipher Block Chaining |
| CE | Cryptographic Erase |
| CNSA | Commercial National Security Algorithm |
| CNSS | Committee on National Security Systems |
| CNSSD | Committee on National Security System Directive |
| CNSSI | Committee on National Security Systems Instruction |
| CNSSP | Committee on National Security Systems Policy |
| COTS | Commercial Off-the-Shelf |
| CP | Capability Package |
| CR | Configuration Requirement |
| CSfC | Commercial Solutions for Classified |
| DAR | Data-at-Rest |
| DEK | Data Encryption Key |
| DIT | Data in Transit |
| DRBG | Deterministic Random Bit Generator |
| DSA | Digital Signature Algorithm |
| ECC | Elliptic Curve Cryptography |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EUD | End User Device |
| FE | File Encryption |
| FE EP | File Encryption Extended Package |
| FEK | File Encryption Key |
| FDE | Full Disk Encryption |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Acronym | Definition |
|---------|---|
| FIPS | Federal Information Processing Standards |
| GCM | Galois/Counter Mode |
| GD | Requirements of Use and Handling of Solutions |
| HF | HWFDE and FE |
| HS | HWFDE and SWFDE |
| HWFDE | Hardware Full Disk Encryption |
| IA | Information Assurance |
| IAVA | Information Assurance Vulnerability Alert |
| ICD | Intelligence Community Directive |
| ICT | Information and Communication Technology |
| IETF | Internet Engineering Task Force |
| ISSO | Information System Security Officer |
| ISV | Independent Software Vendor |
| JIMS | Joint Incident Management System |
| KEK | Key Encryption Key |
| LF | Lost and Found |
| MDF | Mobile Device Fundamentals |
| MicroSD | Micro Secure Digital Card |
| MoA | Memorandum of Agreement |
| NAS | Network Area Storage |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NSS | National Security Systems |
| NTISSI | National Telecommunication and Information Systems Security Instruction |
| O&M | Operations and Maintenance |
| ODNI | Office of the Director of National Intelligence |
| OEM | Original Equipment Manufacturer |
| OPSEC | Operational Security |
| OS | Operating System |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Acronym | Definition |
|---------|--|
| PBE | Pre-Boot Environment |
| PMO | Project Management Office |
| PE | Platform Encryption |
| PF | PE and FE |
| POC | Point of Contact |
| PP | Protection Profile |
| PS | Product Selection |
| PUB | Publication |
| RFC | Request for Comment |
| RA | Risk Assessment |
| RAM | Random Access Memory |
| RM | Removable Media |
| RPG | Random Password Generation |
| SA | Security Administrator |
| SAN | Storage Area Network |
| SC | Supply Chain |
| SCI | Sensitive Compartmented Information |
| SCRM | Supply Chain Risk Management |
| SED | Self-Encrypting Drive |
| SF | SWFDE and FE |
| SHA | Secure Hash Algorithm |
| SIPRNet | Secret Internet Protocol Router Network |
| SR | Solution Requirements |
| SSD | Solid State Drive |
| SW | Software |
| SWFDE | Software Full Disk Encryption |
| T&E | Test and Evaluation |
| TR | Test Requirements |
| TS/SCI | Top Secret/Sensitive Compartmented Information |
| UEFI | Unified Extensible Firmware Interface |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| Acronym | Definition |
|---------|---|
| USB | Universal Serial Bus |
| XEX | XOR Encrypt XOR |
| XOR | Exclusive OR |
| XTS | XEX-based tweaked-codebook mode with cipher text stealing |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



APPENDIX C. CSfC INCIDENT REPORTING TEMPLATE

| | |
|--|--|
| CSfC Incident Reporting Template | |
| Point of Contact (POC) name, phone, email: | |
| Alternate POC name, phone, email: | |
| | |
| CSfC Registration Number: | |
| Classification level of affected system: | |
| Name of affected network(s): | |
| | |
| Affected component(s) manufacturer/vendor: | |
| Affected component(s) model number: | |
| Affected component(s) version number: | |
| | |
| Date and time of incident: | |
| Description of incident: | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | |
|--|--|
| Description of remediation activities: | |
| Is Technical Support from NSA Requested? (Yes/No) | |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



APPENDIX D. PASSWORD/PASSPHRASE STRENGTH PARAMETERS

This appendix provides password and passphrase parameters for use in DAR products to address attacks directly based on the strength of the password or passphrase. It describes what factors provide strength to passwords and passphrases and sets a minimum bar for use.

Strength

Entropy is used as a measure of strength for passwords and passphrases. According to NIST SP800-63-2, *Electronic Authentication Guideline*, entropy is a measure of the amount of uncertainty that an attacker faces to determine the value of the secret. Entropy is usually stated in bits; for example, an unpredictable password with 10 bits of entropy would have 2^{10} or 1,024 possible combinations. The greater the number of possible combinations, the greater the amount of time on average it will take an attacker to find the correct password or passphrase.

Random vs. User Generated

Passwords and passphrases can either be generated randomly or chosen by the user. A randomly generated value has the benefit that it will provide an objective amount of entropy, but can be difficult for a user to remember. A user generated value may be easier to remember, but may be predictable, therefore, lowering the entropy calculation reducing the strength of the password or passphrase. There are many suggested methods for the user generation of passwords; more information on these can be found in NIST SP800-118, *Guide to Enterprise Password Management*. These methods attempt to reduce the predictability while maintaining length and memorability, but because they are user chosen they are all still at risk of being predictable. If the password or passphrase is predictable, an attacker could try a much shorter list of common or personal values reducing the average time to find the correct password or passphrase. The most effective way to ensure the password or passphrase has an appropriate amount of entropy is by applying random generation. The remainder of this appendix addresses random generation.

Randomly Generated Passwords

The strength of a password is determined by the character set and the length. The character set describes the group of unique characters that may be chosen to create the password, such as numbers, lower case letters, upper case letters, special characters, etc. The length simply describes the number of characters chosen.

Randomly Generated Passphrases

The strength of a passphrase is determined by the number of words in the passphrase and the number of words in the word list; the pool of unique words that can be chosen for the passphrase. The word list can be adjusted by the properties of the words it includes, such as minimum word length, maximum word length, and complexity (includes factors such as the difficulty of the word, capitalization, character substitutions, etc.) per word. Each property has a tradeoff between strength and usability. A minimum



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



word length of four is recommended to maintain the effectiveness of the passphrase. This is based on entropy per word from a word list ranging from 10,000 to 450,000 and entropy per character from a character set of 26. This ensures the entropy per set of characters of a given word is greater than the entropy provided selection of a word from the word list.

Assumptions

The product is assumed to meet one of the DAR protection profiles. All password and passphrase conditioning assumes salting is performed, making pre-computed attacks infeasible. A salt is a random value that is used in a cryptographic process to ensure that the results of the computations for one instance cannot be reused by an attacker. The product is assumed to be kept up to date and protection mechanisms used in calculations cannot be bypassed.

Minimum Strength Calculations

The password generation tool is available at csfc_register@nsa.gov and should be used to generate random passwords and passphrases. It will be distributed with usage instructions. The default strength is set to 160 bits, this may be set lower, but shall not be set below 112 bits. If using custom word lists or character sets, Table 21 and Table 22 show the required minimum length of a password and passphrase given a set of characters or words. The user must define the size of the character set or word list they will use. To use the tables, find the value that is less than or equal to your character set (or word list) size in the Character Set Size (or Word List Size) column and the corresponding value in the Minimum Password Length (or Minimum Passphrase Length) column for that row reflects the minimum password (or passphrase) length that shall be used.

Table 21: Randomly Generated Minimum Password Length

| Randomly Generated Passwords | |
|------------------------------|-------------------------|
| Character Set Size | Minimum Password Length |
| 75 | 16 |
| 58 | 17 |
| 47 | 18 |
| 38 | 19 |
| 32 | 20 |
| 27 | 21 |
| 23 | 22 |
| 21 | 23 |
| 18 | 24 |
| 16 | 25 |
| 15 | 26 |
| 13 | 27 |
| 12 | 28 |
| 11 | 29 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | |
|----|----|
| 10 | 30 |
|----|----|

Table 22: Randomly Generated Minimum Passphrase Length

| Randomly Generated Passphrases | |
|--------------------------------|---------------------------|
| Word List Size | Minimum Passphrase Length |
| 1000000 | 5 |
| 100000 | 6 |
| 20000 | 7 |
| 6000 | 8 |
| 2200 | 9 |
| 1000 | 10 |

User-generated passwords should follow local policy with a minimum of 16 characters. User generated passphrases should follow local policy with a minimum of 5 words.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



APPENDIX E: CONFIGURATION GUIDANCE

A number of the DAR requirements listed in the main body of this CP might require additional background information in order to be fully understood by clients who are using them as the basis for preparing Registration Packages for CSfC solutions. The list that follows includes the additional information that we anticipate customers are seeking in order to complete preparing the Registration Packages. If there are questions about requirements that are not discussed in this list, please submit the questions to us and we will respond to them and add them to future updates of this CP.

| REQUIREMENT | CLARIFICATION |
|---|---|
| DAR-SR-1: Default accounts, passwords, community strings, and other default access control mechanisms for all components shall be changed or removed. SF, PF, HF, HS; T=O | Not all products will have defaults. If the product does not have a default no action is needed for compliance with this requirement. If defaults do exist vendors are required to provide guidance on how to change their authentication factors during their protection profile validation. Please refer to NIAP's compliant product list, select your component, and view the Administrative Guidance document. |
| DAR-SR-6: The AO shall provide procedures for performing CE. HF, HS, PF, SF; T=O | Vendors are required to provide guidance on how to perform a cryptographic erase of the encrypted data, this may also be referred to as changing the DEK or TSF Wipe, during their protection profile validation. Please refer to NIAP's compliant product list, select your component, and view the Administrative Guidance document. |
| DAR-CR-1: Default encryption keys shall be changed. SF, PF, HF, HS; T=O | Not all products have default encryption keys. If the keys are generated upon provisioning no action is needed for compliance with this requirement. If default encryption keys do exist, please follow the guidance in DAR-SR-6 to perform a cryptographic erase along with any other vendor guidance provided. |
| DAR-CR-3: DAR components shall use algorithms for encryption selected from Table 1 that are approved to protect the highest classification level of the data. SF, PF, HF, HS; T=O | Not all products allow for changing the algorithms or key sizes used. If more than one is supported the vendor is required to provide guidance for selecting those options. Please refer to NIAP's compliant product list, select your component, and view the Administrative Guidance document. If no options are listed you can confirm vendor algorithm and key size selection in the Security Target document, which is posted on the NIAP page |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | |
|---|--|
| DAR-CR-4: Each DAR component shall prevent further authentication attempts after a number of failed attempts defined by the AO. SF, PF, HF, HS; O | <p>Vendors may not include this functionality in their product, however they may include other non-configurable mitigations.</p> <p>For full disk encryptors, vendors are required to provide one of the following options: Cryptographic erase, forced delay between attempts, or institute a block after a number of consecutive attempts. If your FDE consists of two products, these settings are required for the EE and optional for the AA. The vendor is required to provide guidance for any configurable limits. Please refer to NIAP's compliant product list, select your component, and view the Administrative Guidance document. For information on the selection the vendor made please refer to the Security Target document.</p> <p>For file encryptors, vendors are not required to provide this functionality. Refer to any guidance provided by the vendor.</p> <p>For platform encryption products, vendors are required to implement throttling between authentication attempts. There is no configuration needed for this. The vendor is also required to provide for a cryptographic erase of all protected data, upon a configurable number of failed authentication attempts. The vendor is required to provide guidance on how to configure the number of attempts. Please refer to NIAP's compliant product list, select your component, and view the Administrative Guidance document.</p> |
| DAR-CR-5: Each DAR layer shall perform a CE after a number of consecutive failed logon attempts as defined by the AO. SF, PF, HF, HS; O | Please refer to the guidance given in DAR-CR-4. |
| DAR-CR-10: All CSfC components shall be implemented (configured) using only their NIAP-approved configuration settings. SF, PF, HF, HS; T=O | Please refer to NIAP's compliant product list, select your component, and view the Administrative Guidance document for assistance in configuring the product into a compliant state. |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | |
|--|--|
| <p>DAR-CR-11: Users shall be restricted to designated user folders. SF, HF; T=O</p> | <p>There are multiple ways to accomplish this requirement depending on the OS and software used; any method is acceptable. Here are common ways to accomplish this on the most used OSs. For all restricted directories do the following:</p> <p>Linux: Run the Nautilus file browser, right click the folder, and select Properties. In the Permissions tab change the Access dropdown to Read Only for all end users, then select Change.</p> <p>Mac: Select the folder, select File, click the arrow next to the gear icon to display further options, select Get Info, and click the drop down for sharing and permissions (may have to scroll all the way to the bottom down to see this). For all end users and groups on the device: Select the user or group and choose Read Only. Then select the gear icon and apply all changes. For additional information please see this page: https://support.apple.com/kb/PH18894?locale=en_US&viewlocale=en_US</p> <p>Windows: Right click on the folder, select Properties, and select the Security tab. For all end users and groups on the device: Select the user or group, check the Deny box for the write permission and then click Apply. For additional information please see this page: https://technet.microsoft.com/en-us/library/bb456977.aspx</p> |
| <p>DAR-SW-3: The SWFDE shall be configured to use one of the following authentication options:</p> <ul style="list-style-type: none">· A randomly generated passphrase that meets the minimum strength set in Appendix D. Password/Passphrase Strength Parameters or· A randomly generated password that meets the minimum strength set in Appendix D. Password/Passphrase Strength Parameters or· A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token or· Any combination of the above. SF, HS; T=O | <p>Reference password tool, reference multi-authentication section.</p> |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | |
|--|--|
| DAR-FE-2: The FE product shall use one of the following authentication options: · A randomly generated or user generated passphrase or password defined by the AO that meets minimum strength set in Appendix D, Password/Passphrase Strength or · An external smartcard or software capability containing a software certificate with RSA or Elliptic Curve Cryptography (ECC) key pairs per Table 1. SF, PF, HF; T=O | Reference password tool, reference multi-authentication section. |
| DAR-PE-1: The PE shall enable the “wipe sensitive data” management function for imported or self-generated keys/secrets and/or other classified data. PF; T=O | Vendors are required to provide guidance on how to perform the “wipe sensitive data” management function; this may also be referred to as TSF Wipe, during their protection profile validation. Please refer to NIAP's compliant product list, select your component, and view the Administrative Guidance document. |
| DAR-PE-5: The PE shall use the following for authentication: - A minimum of a four-character, case sensitive alphanumeric password with the length and complexity as defined by the AO, or - A passphrase with the length and complexity as defined by the AO. PF T=O | Reference password tool, reference multi-authentication section. |
| DAR-HW-3: The HWFDE shall be configured to use one of the following authentication options: · A randomly generated passphrase or password that meets the minimum strength set in Appendix D, Password/Passphrase Strength Parameters or · A randomly-generated bit string equivalent to the cryptographic strength of the DEK contained on an external USB token or · A combination of both of the above. HF, HS; T=O | Reference password tool, reference multi- authentication section. |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | |
|---|---|
| DAR-EU-9: The Security Administrator (SA) shall disable system power saving states on EUDs (i.e., sleep and hibernate). SF, HF, HS; T=O | <p>There are multiple ways to accomplish this requirement depending on the OS and software used; any method is acceptable. Here are common ways to accomplish this on the most used OSs.</p> <p>Linux: Please refer to vendor guidance on your specific distribution.</p> <p>Mac: Open Apple menu, select system preference, and select Energy Saver. For all power plans: Drag to slider for computer sleep to Never for sleep. Display sleep does not need to be changed.</p> <p>Windows: Open control panel. Select small icons in the top right, then select power options. For all power plans: Select Change Plan Settings, select Change Advanced Power Settings, expand the sleep list and set Sleep and Hibernate to Disabled.</p> |
| DAR-EU-10: The EUD shall power off after a period of inactivity defined by the AO. SF, HF, HS; T=O | <p>There are multiple ways to accomplish this requirement depending on the OS and software used, any method is acceptable. Here are common ways to accomplish this on the most used OSs.</p> <p>Linux: Please refer to vendor guidance on your specific distribution.</p> <p>Mac: This function must be provided by third party software or running a script.</p> <p>Windows: Open task scheduler, select create task. Under the general tab: Fill in a name. Select run whether user is logged on or not. Make sure run with highest privileges is checked. Under the triggers tab: Click new, select daily, then select ok. Under the actions tab: click new and enter shutdown in the program/script box. Enter /l and /f under the add arguments (optionally) box. Under the conditions tab: Check the box for start the task only if the computer is idle for and Under the settings tab: Check the box if the task fails restart every time and select an increment shorter than the AO defined period. Uncheck the box start the task only if the computer is on AC power. Under the attempt to restart up to box enter 999.</p> |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | |
|---|--|
| DAR-EU-14: System folders shall have user write permissions disabled unless authorized by an administrator. SF, HF; T=O | Please refer to guidance on DAR-CR-11 and ensure end users are restricted from writing to system folders. |
| DAR-EU-20: The BIOS shall be configured to require a password before continuing the boot process. HF, HS, SF; O | This is a password to continue the boot process, creating a password prompt before the FDE and/or OS login. Not all motherboards support this feature. Generally the first screen will indicate which button is used to change BIOS/UEFI settings; if not please refer to product documentation. Once in the settings, browse for an option to require a password to continue the boot process and enable it. The password does not need to be strong, the absence of the password would indicate tampering. |
| DAR-EU-21: All DAR FDE components shall be cryptographically erased before being provisioned again. HF, HS, SF; T=O | Please refer to DAR_SR_6 guidance on how to perform a cryptographic erase. |
| DAR-EU-22: All DAR components shall be cryptographically erased before being provisioned again. PF; O | Please refer to DAR_SR_6 guidance on how to perform a cryptographic erase. |
| DAR-EU-24: The EUD shall enable the BIOS/UEFI password. HF, HS, SF; O | This is a password that is required before allowing access to change BIOS/UEFI settings. Not all motherboards support this feature. Generally the first screen will indicate which button is used to change BIOS/UEFI settings; if not please refer to product documentation. Once in the settings, browse for an option to set a BIOS/UEFI password. |
| DAR-EU-26: Each EUD shall be personalized by the end user. (This should not violate any other security features.) HF, HS, PF, SF; O | Personalization means making device changes specific to each end user that would be noticed before both layers are authenticated. This can include stickers, markings, wallpapers, etc. |
| DAR-KM-3: The DAR solution shall disable all key recovery mechanisms. SF, PF, HF, HS; T=O | If the product supports key recovery mechanisms they are required to state how to disable those mechanisms in their documentation. Please refer to NIAP's compliant product list, select your component, and view the Administrative Guidance document. |
| DAR-LF-5: EUDs shall use boot integrity verification technology. HF, HS; T=O | This requirement is based on device acquisition. Not all devices support these features. The specific features will have to be discussed with the device vendor and then configured according to that vendor's specifications. |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | |
|---|---|
| DAR-LF-6: The EUD shall enable the BIOS/Unified Extensible Firmware Interface (UEFI) password. HF, HS; T=O | Please refer to guidance on DAR-EU-24 to enable a BIOS/UEFI password. |
| DAR-LF-12: Each EUD shall be personalized by the end user. (This should not violate any other security features.) HF, HS, PF; T=O | Please refer to DAR-EU-26 to personalize devices. |

APPENDIX F: CONTINUOUS PHYSICAL CONTROL

Since the NSA requires that implementing organizations define the circumstances in which an EUD that is part of the solution is considered outside of the continuous physical control of authorized users (i.e., "lost"), Authorizing Officials (AO) will define "continuous physical control", and that definition should align with the intended mission and threat environment for which the solution will be deployed. Organizations must also define the circumstances in which an EUD that is a part of that organization's solution is to be considered recovered back into the continuous physical control of authorized users (i.e., "found").

In order to provide some guidance to clients who may not have experience with handling continuous physical control issues, we have consulted several experienced organizations that have provided examples of the criteria they use to define "continuous physical control". The intent of this is to cite a number of potential generic measures that can be taken as additional Continuous Physical Control guidance in DAR 4.0 without attribution to the source of these measures.

DAR customers have provided several ideas of measures they are considering to deal with particular circumstances. Listed are some of the ideas being considered for handling EUDs:

- Package using clear one-use bags.
- Use tamper evident stickers with recorded unique serial numbers on critical screws.
- Use commercial backpacks with-pick-resistant locks.
- Lock in automobile glove box and lock the car.

Some users currently handle the issue by simply not authorizing the removal of any EUDs from the secure location where they are housed.

Continuous Physical Control Examples:

(U) To assist in the development of well thought out definitions of continuous physical control, segments of good definitions used by previous registrations have been provided. These examples should be reviewed to ensure that the definition given for a registration follows the intent of the requirement.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



Traveling with EUDs. Commands will create local policy to address specifics on traveling with EUDs, to include outside the continental U.S. (OCNUS) locations, IAW local security procedures.

The following general actions apply while traveling with EUDs:

a. Prior to travel:

- (1) Do not take your device if you can do without it.
- (2) Do not take information you do not need, including sensitive contact information.
- (3) Ensure that the latest, most current, up-to-date antivirus protection, spyware protection, OS security patches, and a personal firewall have been pushed and enabled by the responsible Information Technology (IT) support.
- (4) Disable infrared ports and features you do not need.

b. During travel:

- (1) Keep the EUD under physical control at all times when traveling.
- (2) Never place the EUD in checked luggage.
- (3) Never store the EUD in an airport, train station, bus station, or any public locker.
- (4) If leaving the EUD in a vehicle, lock the EUD or keep it out of sight.
- (5) Do not leave EUDs unattended unless required activities demand so. In the event that they must be unattended, stow them securely and out of sight after removing the battery and SIM card. Keep the battery and SIM card under control at all times to maintain the protection of its information.
- (6) Avoid leaving the EUD in a hotel room.
- (7) Be prepared for airport security checks. Have the EUD's batteries charged or a power cord handy to demonstrate if necessary that it is functional.
- (8) Heighten vigilance at any security or luggage-scanning checkpoint. Place EUD on the conveyer belt only after the belongings of the person ahead of you have cleared the scanner. If delayed, keep the EUD in view.
- (9) Exercise diligence when traveling in foreign countries because criminals or local intelligence may target the EUD for the information it contains.
- (10) Do not display any sensitive information on the EUD screen when in any public place (such as an airport terminal, train or bus station, airplane, train, bus, or taxi).
- (11) Terminate connections when not using them.
- (12) If the device or information is stolen, report it immediately to your home organization and the local U.S. embassy or consulate.

c. Return from travel:

- (1) Change the password.
- (2) Have your command or unit examine the device for the presence of malicious software.



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



APPENDIX G. REFERENCES

| | | |
|------------------------------------|--|---------------|
| CNSSD 505 | <i>CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)</i> | March 2012 |
| CNSSI 1253 | <i>CNSS Instruction No. 1253, Security Categorization and Control Selection for National Security Systems</i> | March 2014 |
| CNSSI 4004 | <i>Committee on National Security Systems Instruction (CNSSI) No. 4004 Destruction and Emergency Protection Procedures for COMSEC and Classified Material</i> | August 2006 |
| CNSSI 4009 | <i>CNSSI 4009, Committee on National Security Systems (CNSS) Glossary</i> www.cnss.gov/Assets/pdf/cnssi_4009.pdf | April 2015 |
| CNSSP 15 | <i>CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems</i> | October 2012 |
| CSfC Components List | <i>CSfC Components List</i> Available on the CSfC web page http://www.nsa.gov/ia/programs/csfc_program | May 2014 |
| CSfC Incident Reporting Guidelines | <i>CSfC Incident Reporting Guidelines</i> Available on the CSfC web page http://www.nsa.gov/ia/programs/csfc_program | June 2014 |
| FE Extended Package | <i>File Encryption Extended Package.</i> www.niap-ccevs.org/pp | November 2014 |
| FIPS 140-2 | <i>Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules</i> | May 2001 |
| FIPS 180-4 | <i>Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)</i> | March 2012 |
| FIPS 186-4 | <i>Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), (Revision of FIPS 186-2, June 2000)</i> | July 2013 |
| FIPS 197 | <i>Federal Information Processing Standard 197, Advanced Encryption Standard (AES)</i> | November 2001 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



| | | |
|---|---|----------------------|
| FIPS 201-2 | <i>Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication</i> http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chnq1.pdf | August 2013 |
| MDF PP | <i>Mobile Device Fundamentals Protection Profile.</i> www.niap-ccevs.org/pp | September 2014 |
| NIST SP 800-111 | <i>NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices</i> | November 2007 |
| NIST SP 800-131A | <i>NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths. E. Barker.</i> | January 2011 |
| NIST SP 800-132 | <i>Recommendation for Password-Based Key Derivation</i> | December 2010 |
| NIST SP 800-147 | <i>NIST Special Publication 800-147, BIOS Protection Guidelines. D. Cooper, et. al.</i> | April 2011 |
| NIST SP 800-56A | <i>NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. E. Barker, D. Johnson, and M. Smid</i> | March 2007 |
| NIST SP 800-56B | <i>NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography. E. Barker, et. al.</i> | August 2009 |
| NIST SP 800-56C | <i>NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion. L. Chen.</i> | November 2011 |
| NIST SP 800-63-2 | <i>NIST Special Publication 800-63-2, Electronic Authentication Guideline</i> | August 2013 |
| NSA CNSA | <i>NSA Guidance on CNSA Cryptography</i> http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml | No Date Specified |
| NSA/CSS Policy Manual 9-12 Storage Device Sanitization | https://www.nsa.gov/ia/files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf | December 2014 |



Data at Rest Capability Package



INFORMATION ASSURANCE
BY THE NATIONAL SECURITY AGENCY



SW FDE PP

Software Full Disk Encryption Protection Profile. www.niap-ccevs.org/pp

February
2013